Sygate Personal Firewall Pro User Guide

Sygate Technologies, Inc.
6595 Dumbarton Circle
Fremont, CA 94555
http://www.sygate.com

Sygate® Personal Firewall Pro™ User Guide

Note: Sygate® is a registered trademark of Sygate Technologies, Inc. Microsoft is a registered trademark, and Windows, Windows ME, Windows 2000, Windows NT, Windows XP, and Windows 95/98 are trademarks of Microsoft Corporation. All other companies and product names are trademarks or registered trademarks of their respective holders.

Table of Contents

Sygate® Personal Firewall Pro™ User Guide Version 2.0

Introduction

Sygate Personal Firewall Pro is comprehensive computer protection from hackers and other malicious intruders.

INTRODUCING SYGATE® PERSONAL FIREWALL PRO™

Thank you for choosing **Sygate Personal Firewall Pro** for your Internet security needs. **Sygate Personal Firewall Pro** is one of the simplest, most powerful tools that you can find today to protect you, and your computer, from unwanted intruders.

Bi-Directional Defense

As a bi-directional intrusion defense system, **Sygate Personal Firewall Pro** ensures that your personal computer is protected from external intrusion attempts while simultaneously preventing unauthorized access from your computer to a network. **Sygate Personal Firewall Pro** is a must-have security measure for any PC or lap-top that connects to any network, especially the public Internet.

Any Location

No matter where you use your computer, whether remotely or from behind a corporate firewall, whether using a dial-up modem or an always-on broadband Internet connection, **Sygate Personal Firewall Pro** gives you complete confidence that precious business, personal, and financial data is safe and secure from malicious hackers, cracks, and Script Kiddies. If that isn't enough, **Sygate Personal Firewall Pro** includes advanced active-scan vulnerability assessment to pinpoint weaknesses and fine-tune security policies.

Friendly and Configurable

Sygate Personal Firewall Pro, while highly configurable for power users, is easy to use. Even inexperienced web-surfers can enjoy easy Internet access with full confidence and security. **Sygate Personal Firewall Pro** quickly installs on your system and automatically detects your Internet connection and settings. After installation, you are ready to go, with complete protection for all of your networking needs.

ABOUT THIS DOCUMENT

This document is an overview of the installation, deployment, and use of **Sygate**

Personal Firewall Pro, a Sygate® Technologies software. This document is written for a typical computer user. Questions regarding the content of this document can be emailed to **documentation@sygate.com.**

Assumptions

This guide assumes that the user is familiar with the basic functioning of Windows operating systems, and standard Windows items, such as buttons, menus, toolbars, windows, etc.

Further, this guide assumes that the user has an Internet connection, whether through a private network, DSL connection, dial-up modem, or some other form of connection.

Terms

Depending on the kind of computing system that you use, you may connect to the Internet through a local area network (LAN), DSL, dial-up modem, or any number of other methods. The term "network connection" is used to refer to all of these different connection methods.

Conventions

red, Helvetica bold font	**product name and abbreviation (Sygate Personal Firewall Pro, SPF Pro)**
bold font	**keyboard and on-screen keys, windows, screens, fields, pull-down lists, tabs**
courier	all command lines entered in MSDOS
gray	security levels in **Sygate Personal Firewall Pro**
italics	*used to emphasize important points*

Support

Questions regarding the use of the product can be emailed to our support team through our web site at http://www.sygate.com, under the Support menu.

How Firewalls Work

If you are already familiar with firewalls and the way they work, you can skip this section. However, if this is your first time using **Sygate Personal Firewall Pro** (or any firewall, for that matter), this section might help you to better understand the behavior of your firewall, and how it works to protect you.

There are a number of ways in which you can protect your computer from potential intruders, and installing a powerful computer firewall is one of the best methods. Firewalls come in different forms. Some are software applications, like **Sygate Personal Firewall Pro**. Others are hardware devices, and some are a combination of hardware and software.

All firewalls have the common function of watching information that flows into your computer. The unfortunate truth is, in most cases, it isn't enough to merely look at incoming data. Often, firewalls aren't aware that incoming data is bad until it has actually triggered a problem.

That is why **Sygate Personal Firewall Pro** takes a comprehensive approach to computer security. **Sygate Personal Firewall Pro** ***monitors*** all traffic attempting to use your network connection, ***analyzes*** the traffic for unusual attributes, ***responds*** to the traffic based on the analysis, and ***reports*** the interactions in detailed log files. Finally, **Sygate Personal Firewall Pro** offers links to Sygate® Online Services, which ***assesses*** your system for possible security holes, allowing you find weak security areas before a hacker finds them.

Sygate Personal Firewall Pro is Your Elite Security Squad...

Imagine you own an nightclub. Not just any club, but an expensive, exclusive club, where the clientele is famous, the chandeliers immense, and the dance floor is imported Italian marble: the kind of place that supermodels vie to get in to. Think Studio 54 meets Spago. Not only would you hire the best cooks, waiters, and bartenders available, but you would also hire the best security possible, to ensure the safety of your guests and customers.

You would most likely keep burly, stern bouncers at every entrance, extensive security cameras throughout the building, and well-trained security guards to monitor the building's interior, to protect your guests from possible harassment from univited guests.

You might not think of your computer as an exclusive night club, but you should. It might not lead you into *direct* contact with supermodels, but it contains all sorts of precious information, files, and data, that are constantly at risk from outside intrusion. Like a popular nightclub, your computer is always being eyed by people who want to break in and crash the party, so to speak.

What would you do if suddenly, all the files on your computer disappeared? Worse yet, what if private information, such as credit card numbers, were stolen and used by a hacker? You owe it to yourself and your computer to hire the best security team available to protect you and your data from uninvited guests. It's true: your computer is an exclusive nightclub and your network connection is the front door.

Sygate Personal Firewall Pro functions like a set of burly bouncers and security guards, monitoring every guest that attempts to get into or out of your nightclub.

Monitor

When any "guest" attempts to access your network connection, your computer's bouncer, **Sygate® Personal Firewall Pro ™**, examines it carefully.

A "guest" would be any **packet** of information that attempts to use your network connection (or modem). **Sygate Personal Firewall Pro** uses *application-based security rules*, meaning that it examines the application being used to send the packet. An incoming or outgoing packet could be a legitimate application, such as a web browser or a media streaming device, or it could be a potentially hazardous program, like a virus or a Trojan horse, attempting to make use of other applications in order damage or steal your personal files and information.

Sneaking Suspicions

Some of the most dangerous intrusion methods use a technique known as "masquerading" in order to sneak past security systems. "Masquerading" is when an intrusive program, such as a Trojan horse, *pretends to be a legitimate program* in order to gain access to a computer or network. Recalling the night club analogy, imagine that an uninvited guest manages to look like a celebrity by donning a mask and renting a limousine for the evening. If this guest manages to fool security, they might gain entrance to the night club.

This is the same strategy used by malicious intrusion programs. Once such a program manages to sneak past a firewall by pretending to be a safe program, it is normally free to wreak havoc on your computer and computer network.

For this reason, **Sygate Personal Firewall Pro** uses bi-directional scans to examine each guest using checksum. Checksum is an error-detection scheme that assigns a numerical value to a packet of data based on the amount of data in the packet. Each application has its own value, and **Sygate Personal Firewall Pro** checks each *incoming* and *outgoing* application for this value. Every time an application tries to access your network connection, either to enter or leave your computer, its checksum value must match its previous checksum noted by **Sygate® Personal Firewall Pro ™**. If the values do not match, **Sygate Personal Firewall Pro** will notify you of the difference with a pop-up message (for further information on pop-up messages, see "Why Did I Get a

Pop-Up Message?", starting on page 20).

Eyes in the Back of Your Head

Sometimes, suspicious activity can arise from *inside*. In a night club, a seedy type of character might have slipped into a club *before the security team arrived.* This intruder might try to damage the club's interior, or try to steal something and slip away unnoticed.

Likewise, computers can already contain harmful programs like Trojan horses before a firewall is installed - *which is why* Sygate® Personal Firewall Pro , *like a bouncer, is constantly on the look out for any suspicious guest* ***entering*** *or* ***leaving*** *the establishment, through* ***any*** *entrance.* With bi-directional security, Sygate Personal Firewall Pro prevents the loss of valuable information by keeping a sharp eye on your computer's connections.

A good firewall, like a good security guard, watches all ports and windows to make sure that only the good get in, and nothing important gets out.

Analyze

Rather than merely observing guests, a security guard at an exclusive nightclub carefully scrutinizes each guest before deciding whether or not to permit them to enter the establishment. Potential guests have to prove that their name is on the guest list, or that they are old enough to get inside.

Similarly, Sygate Personal Firewall Pro examines every aspect of a potential "guest": Is the appropriate name on the guest list? Has this guest been granted entrance before? Has this guest's appearance changed since the last visit? Does this guest have the appearance of a genuine application or protocol? Where is this guest coming from? What does the guest want? Is there anything suspicious about his or her activity?

Respond

A decision is then made. In the case of a bouncer, a guest can be allowed in, or kicked out. Occasionally, a bouncer might ask the club's manager if the guest should be allowed in.

Sygate Personal Firewall Pro goes through a similar process. In the case of incoming guests, if the guest's name is on the list, and the guest qualifies as legitimate under all specifications, the guest is allowed in.

If the guest isn't on the list, but passes inspection, the firewall will inquire if you, the manager, want to permit the guest to enter. If the guest looks suspicious, or has been denied entrance before, the firewall will immediately deny entrance.

Even if an incoming packet passes through Sygate Personal Firewall Pro, its application is still carefully monitored for unusual behavior. If an application tries to send information out of your computer, Sygate Personal Firewall Pro is there, watching all doorways, preventing the loss of valuable information.

Report

Sygate Personal Firewall Pro has a unique and powerful logging system that records traffic that attempts to use your network connection. Four separate logs track firewall operation, attempted attacks, network traffic, and raw packet data with details such as remote ports and host names, IP addresses, and attack types. These logs can be accessed at any time from the System Tray Icon or main console, and can be configured and consolidated for easy viewing and storage.

Additionally, **Sygate Personal Firewall Pro** offers the option to back trace logged events in the Security and Traffic Logs, and provides the names and addresses of network administrators overseeing computers used in hacking attacks.

Assess

Sygate® Online Services provides six unique scans that determine and report possible weak points in your security so that you can cover them before they are discovered by a hacker (for details on SOS vulnerability assessment, see "Vulnerability Assessment", starting on page 67).

Sygate Personal Firewall Pro is the Best Solution Around

We know you have a variety of firewalls to choose from, and we are confident that you have chosen the best one available. **Sygate Personal Firewall Pro** is the latest and most powerful personal firewall from Sygate® Technologies, Inc.

Sygate Personal Firewall Pro combines vulnerability assessment with configurable application-based bi-directional security to provide you with the utmost in personal computing security.

Installation

Before installing **Sygate Personal Firewall Pro**, please make sure that you have uninstalled all previous versions of **Sygate Personal Firewall Pro.**

Sygate Personal Firewall Pro combines simple installation with user friendly deployment. Before beginning installation, it is required that you exit all other programs that access your network or Internet connection. This includes web browsers, email programs, instant messenger sessions, and media streaming applications (such as Internet radio broadcasts).

Computer Environment Requirements

Minimum System Requirements

- Pentium 133 or equivalent
- 32 MB RAM
- 10 MB free disk space
- At least one network adapter or modem
- TCP/IP protocol installed
- Internet Explorer Version 4.0 or later

Operating Systems (any one or a combination of those listed below)

- Windows 95, 95 OSR1, 95 OSR2, 95 OSR2.5
- Windows 98, 98 Second Edition
- Windows Millennium Edition (ME)
- Windows NT 4.0 Workstation with SP5 or later
- Windows NT 4.0 Server with SP5 or later
- Windows NT 4.0 Terminal Server with SP5 or later
- Windows 2000 Professional, Server, Advanced Server, Data Center
- Windows XP

Supported Internet Connections

- Dial-up modems, ISDN modems, cable modems, DSL, LAN, wireless LAN, DirecPC, StarBand, other wireless or satellite connections

Downloading

1. Make sure that you have completely uninstalled all previous versions of **Sygate**

Personal Firewall Pro.

2. Click the **Sygate Personal Firewall Pro** download link on the Sygate® Technologies, Inc. web site (www.sygate.com).

3. Select the download folder for the **Sygate Personal Firewall Pro** files.

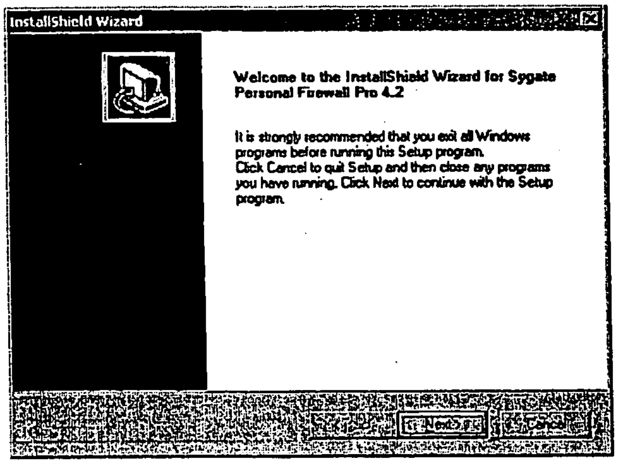
Begin Installing

1. From the specified download folder, open the executable file by clicking on the icon. You may have to unzip the file first. **Sygate Personal Firewall Pro** begins extracting files.

2. If you see the Overwrite Protection message, click **Yes to All.** This indicates that you had an earlier version of **Sygate Personal Firewall Pro** installed on your computer.

3. Next, **InstallShield Wizard** launches and will begin installing **Sygate Personal Firewall Pro.**

4. The **InstallShield Wizard** screen opens, displaying the **Welcome** screen. Click **Next.**



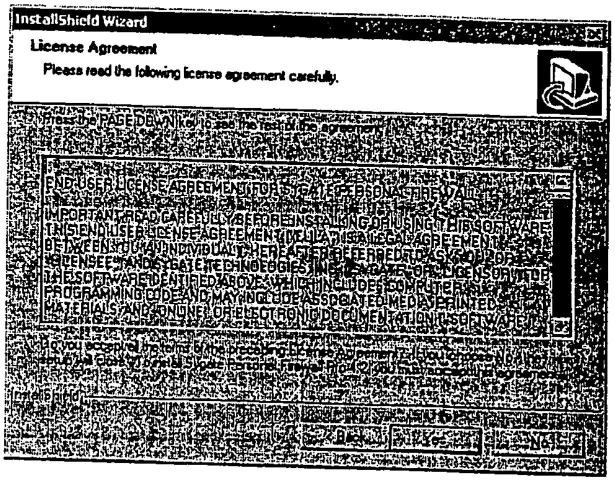
Welcome to the InstallShield Wizard for Sygate Personal Firewall Pro 4.2

It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

InstallShield Welcome Screen

5. Next, the **End User License Agreement** is displayed. Scroll through the Agreement and

read the terms of use for this product. Click **Yes** if you accept the terms.



InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

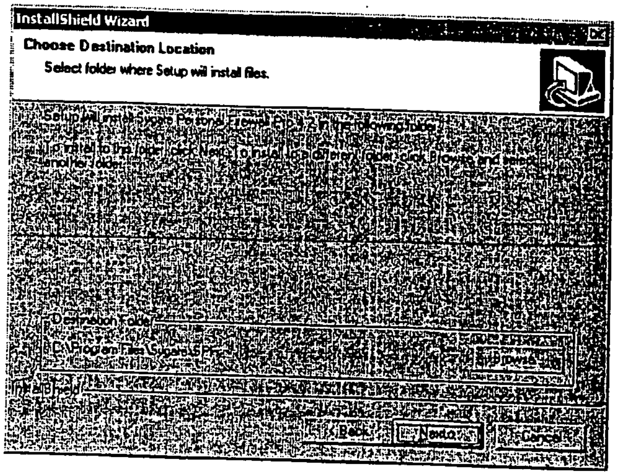
END USER LICENSE AGREEMENT FOR SYGATE PERSONAL FIREWALL [illegible]

IMPORTANT-READ CAREFULLY BEFORE INSTALLING OR USING THIS SOFTWARE. THIS END USER LICENSE AGREEMENT (EULA) IS A LEGAL AGREEMENT BETWEEN YOU (AN INDIVIDUAL, HEREAFTER REFERRED TO AS "YOU" OR [illegible] "LICENSEE") AND SYGATE TECHNOLOGIES INC. (SYGATE OR LICENSOR) FOR THE SOFTWARE IDENTIFIED ABOVE, WHICH INCLUDES COMPUTER [illegible] PROGRAMMING CODE AND MAY INCLUDE ASSOCIATED MEDIA, PRINTED [illegible] MATERIALS, AND "ONLINE" OR ELECTRONIC DOCUMENTATION ("SOFTWARE").

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install Sygate Personal Firewall Pro 2.0, you must accept this agreement.

End User License Agreement

6. Next, the **Destination Location** screen appears. Click **Browse** to select the precise



InstallShield Wizard

Choose Destination Location

Select folder where Setup will install files.

Setup will install Sygate Personal Firewall Pro 2.0 in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

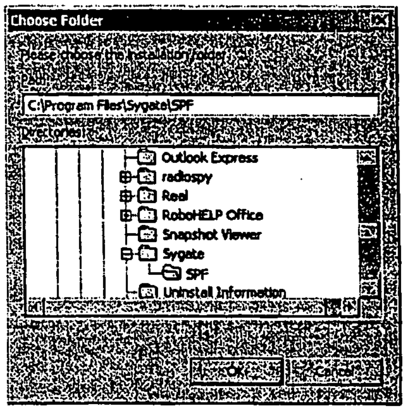
C:\Program Files\Sygate\SPF

Destination Location Screen

location for the installation of **Sygate Personal Firewall Pro**. Select the folder in which

Sygate Personal Firewall Pro will be installed by clicking on the icon so that the folder name is highlighted. Click **OK.**

7. Click **Next** when the **Destination Location** screen reappears, displaying the correct path for the installation of **Sygate Personal Firewall Pro.**



Please choose the installation folder.

Path:

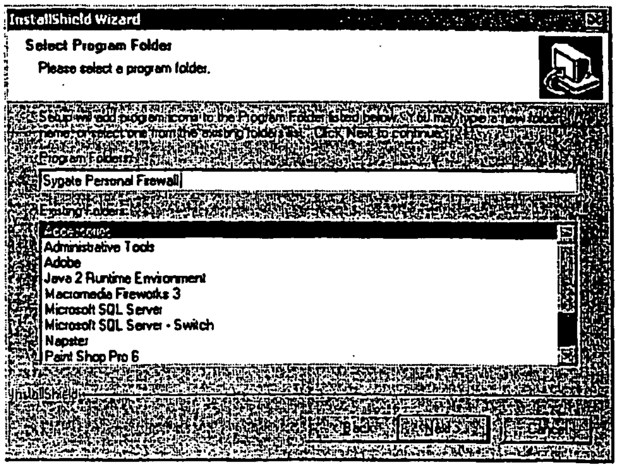
C:\Program Files\Sygate\SPF

Directories:

Outlook Express
radiospy
Real
RoboHELP Office
Snapshot Viewer
Sygate
SPF
Uninstall Information

Select a location for Sygate® Personal Firewall™

8. Select the program folders in which you wish to display **Sygate Personal Firewall** program icons. You may enter a new folder name or select a name from the list.



Select Program Folder

Please select a program folder.

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.

Program Folders:

Sygate Personal Firewall

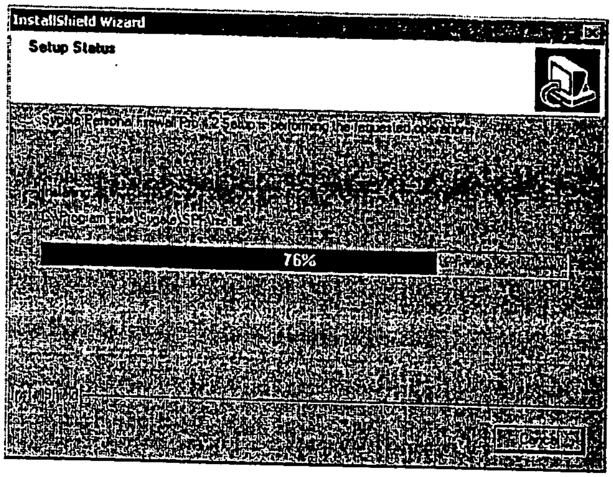
Existing Folders:

Accessories
Administrative Tools
Adobe
Java 2 Runtime Environment
Macromedia Fireworks 3
Microsoft SQL Server
Microsoft SQL Server - Switch
Napster
Paint Shop Pro 6

Select Program Folder

9. Click **Next.**

10. **InstallShield Wizard** completes the installation of **Sygate Personal Firewall Pro.**



InstallShield Wizard

Setup Status

Sygate Personal Firewall Pro 4.2 Setup is performing the requested operations.

[illegible]

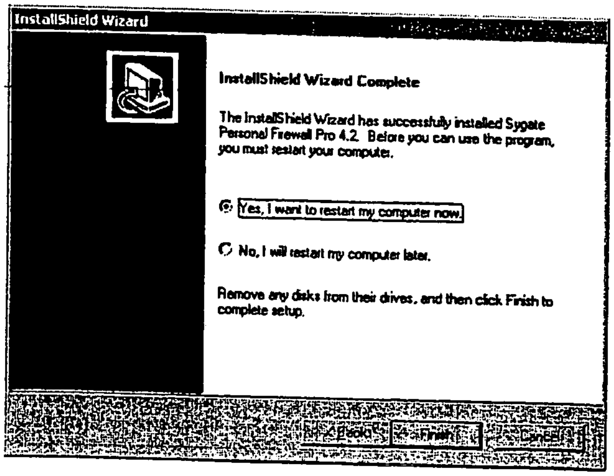
[illegible]Program Files\Sygate\SPF\[illegible]

76%

Installation Completion Window

11. You will see the **System Configuration** message as **Sygate Personal Firewall Pro** completes system configuration.

12. The installation is completed. Select **Yes** and click **Finish** to restart your computer.



InstallShield Wizard

InstallShield Wizard Complete

The InstallShield Wizard has successfuly installed Sygate Personal Firewall Pro 4.2. Before you can use the program, you must restart your computer.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

Install Completed

Registering Sygate® Personal Firewall Pro™

13. Next, the **Registration** window will open, prompting you to register your installation of **Sygate Personal Firewall Pro**. You have the option to register the product immediately or defer registration until another time by using the 30-day trial option.

> We recommend registering your installation of **Sygate Personal Firewall Pro** as soon as possible. Registering the product enables you to receive support from Sygate® Technologies, Inc. You can reach Sygate® Technologies Support via email at support@sygate.com. If you decide to register later, you can always access the registration form from the main console by opening the **Help** menu and selecting **Register...** from this list of options.

Please note that any and all information you provide is kept confidential. Sygate® Technologies, Inc. does not sell or trade customer information with other companies or organizations.

To complete registration, you must purchase **Sygate Personal Firewall Pro** from the Sygate® Technologies web site at http://www.sygate.com. If you have already purchased **Sygate Personal Firewall Pro**, and have the serial number and registration code available, you may register the product. Enter the appropriate information in the fields provided and click the Register Now button, or click the **Try Now** button to take advantage of the **Sygate Personal Firewall Pro** 30-day trial.

Again, please make sure to include a valid email address in the appropriate field. In order to receive email support from Sygate® Technologies, Inc., you must properly register your product.

You're Secure!

After the installation of **Sygate Personal Firewall Pro**, you are protected from hackers and other unwanted intruders immediately, without having to configure anything! Of course, **Sygate Personal Firewall Pro** comes with configurability options that beginning and advanced users alike can use to create security solutions customized to individual needs. But users should rest assured that they are safe and secure with **Sygate Personal Firewall Pro** immediately.

Starting with Sygate Personal Firewall Pro

Using a firewall is like having a body guard installed on your computer.

As discussed, **Sygate Personal Firewall Pro** is always on the look out for suspicious guests entering and leaving your computer through your network or Internet connection. The way in which **Sygate Personal Firewall Pro**'s monitoring affects every day computing will vary from user to user. **Sygate Personal Firewall Pro** shouldn't affect your connection speed (if it does, consult your IT department or Sygate® Technologies support via email at support@sygate.com).

However, you will notice a fair amount of interaction with **Sygate Personal Firewall Pro** initially, until it gets used to your computing style. The first thing you will probably notice is the barrage of pop-up message you receive every time you try to launch a program that uses your modem or network connection.

Why Did I Get a Pop-Up Message?

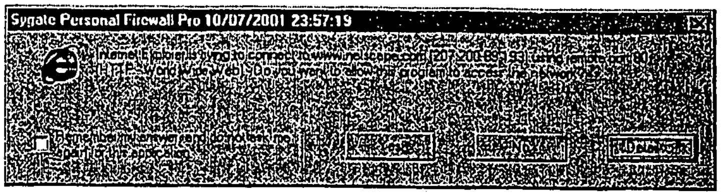
An application-related pop-up message will occur for one of three reasons:

- An application that **Sygate Personal Firewall Pro** has never seen before, or that has been assigned the status of "Ask", is trying to access your network connection.
- An application that normally accesses your network connection has changed, possibly because of a product upgrade.
- **Sygate Personal Firewall Pro** has detected a Trojan horse on your computer.

New Application Pop-up

Imagine that you are sitting at your desk, working on a proposal using standard word processing software. **Sygate Personal Firewall Pro** is running in the background.

Suddenly, the following pop-up message appears on your computer screen.



Sygate Personal Firewall Pro 10/07/2001 23:57:19

Internet Explorer is trying to connect to www.netscape.com [207.200.89.193] using remote port 80 (HTTP - World Wide Web). Do you want to allow this program to access the network?

□ Remember my answer and do not ask me again for this application.

Sygate Personal Firewall Pro Pop-up Message

What Does This Mean?

The information on the pop-up tells you that Microsoft Internet Explorer is trying to access your network connection. The site that Internet Explorer is trying to load is scan.sygatetech.com, which has an IP address of 207.33.111.332. The server (computer) that powers that site is using server port 80. Initially, that might seem like too much information to take in.

Detail

Clicking the **Detail** button opens another information field that contains further details on the connection the application is attempting to establish. Information such as the file name, version, and path are provided. Look at these items to make sure that they match the description of the application that you normally use. The details section should also indicate where the file was initiated: either local (meaning that it was opened on your computer) or remote (meaning that the application was initiated by an outside source). Additionally, the local and remote ports numbers and IP addresses should be provided.

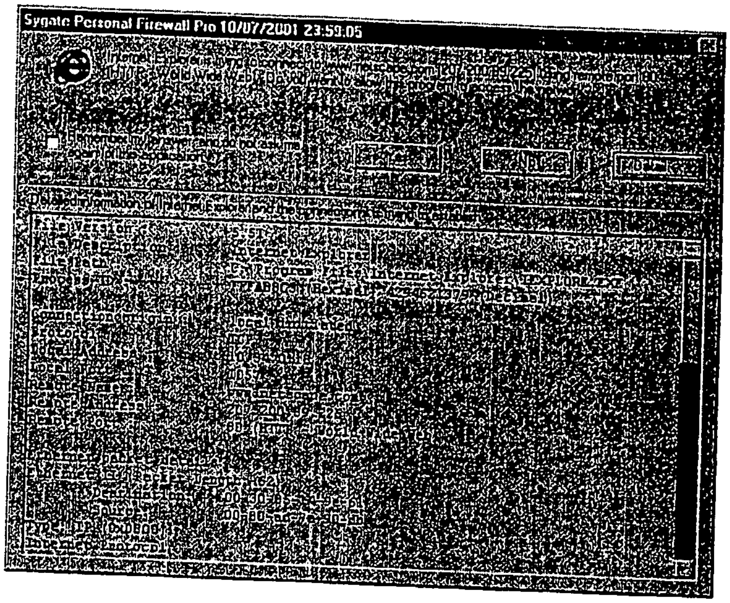
Why Did This Appear?

This pop-up appeared because Microsoft Internet Explorer has been opened, either directly by you, indirectly by you, or by another application.

You might have tried to open Internet Explorer. If so, either this is the first time that you have done so since you installed **Sygate Personal Firewall Pro**, or you have assigned Internet Explorer a status of "Ask", meaning that every time Internet Explorer tries to access your network connection, **Sygate Personal Firewall Pro** will ask you to grant it access (for more information on access status, see "Viewing the Applications List", starting on page 41).

What if you did not directly try to open Internet Explorer? Perhaps you clicked on a link to a web site, or tried to open another program that might use Internet Explorer. You might have clicked the **Test** button on the **Sygate Personal Firewall Pro** main console (for information on testing your firewall, see "Vulnerability Assessment", starting on page 67). If so, your computer will try to open Internet Explorer for you. In such a case, it is probably safe to click **Yes** and allow Internet Explorer to access the network.

What if you didn't open any program or click on any link, and a program suddenly tries to access your network connection? Again, there could be a number of different reasons. However, if you haven't opened any programs that use the application listed on the pop-up message, or can't see any reason why that application should try to access your network connection, it is always safest to say **No**. This might indicate the presence of a Trojan horse on your computer, something that needs to be checked immediately.



Sygate Personal Firewall Pro 10/07/2001 23:59:05

Pop-up Message Application Details

What Should I Do When I Receive a New Application Message?

This kind of message is common when you first start using **Sygate Personal Firewall Pro**. In this particular example, Microsoft Internet Explorer is trying to access a Sygate® Technologies web site at the remote port 80. Most servers use port 80 to send and receive information on the Internet, so this isn't anything unusual.

If you believe that you have triggered this application, it would be safe to click **Yes**. You have the option to tell **Sygate Personal Firewall Pro** to remember your answer in the future. If you check the box marked **Remember my answer, and do not ask me again for this application, Sygate Personal Firewall Pro** will remember your choice, and will act accordingly the next time this application tries to access your network connection.

Should I Select "Yes"?

If you have tried to open an application (such as a web browser) or a program that uses another application to access the Internet (such as a media streaming program) and you feel comfortable granting this application access to your network connection, then you can select **Yes**. The application will then be able to access your network. You can change the status of the application at any time, either in the **Running Applications** field or in the **Applications List**.

Should I Select "No"?

However, if a pop-up message is unexpected, and you can't see any reason why the listed application should try to access your network connection, select **No.** This will assign the access status of **Block**, so that it will be automatically blocked from your network connection any time it tries to gain access. You can change the status of the application at any time, either in the **Running Applications** field or in the **Applications List.**

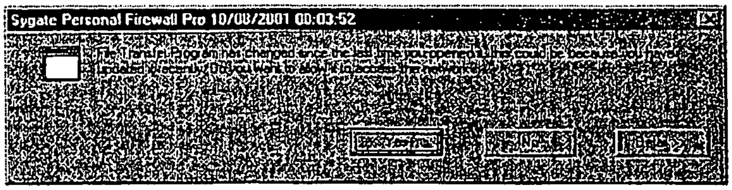
You should also run a virus scan to make sure that you have not inadvertently downloaded a virus or a Trojan horse that could infect your computer files.

Table 1: Pop-ups and Access Status

Click	Check "Remember my answer..." box?	Access Status Assigned
Yes	Yes	**Allow**
Yes	No	**Ask**
No	Yes	**Block**
No	No	**Ask**

Changed Application Pop-up

Occasionally, you might see a pop-up such as the one pictured below.



Sygate Personal Firewall Pro 10/08/2001 00:03:52

File Transfer Program has changed since the last time you opened it. This could be because you have updated it recently. Do you wish to allow it to access the network?

Changed Application Pop-up Message

What Does This Mean?

The application listed on the pop-up message is trying to access your network connection. Although **Sygate Personal Firewall Pro** recognizes the name of the application, something about the application has changed since the last time **Sygate Personal Firewall Pro** encountered it.

Detail

Again, clicking the **Detail** button will provide further information on the application's origins, file name, path, etc.

Why Did This Appear?

This could be because you have upgraded the product recently. **Sygate Personal Firewall Pro** uses checksum to determine the legitimacy of an application, an upgraded version might not pass the checksum test, since a new build or new version of the application is likely to have a different checksum value.

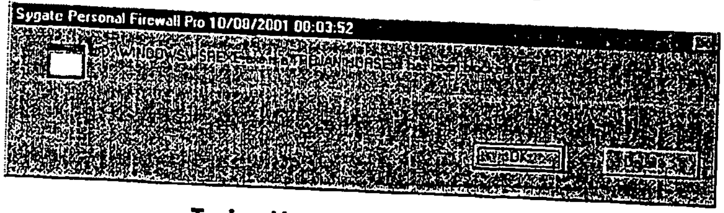
On the other hand, if you have not recently upgraded the application, and see no reason why this message should appear, this could be an instance of a new Trojan horse trying to access your network.

What Should I Do When I Receive a Changed Application Message?

If you have recently upgraded the application mentioned on the pop-up message, it is probably safe to click **Yes** and allow the application network access. However, if you do not think that you have recently upgraded the listed application, you should select **No** and run an anti-virus software program or, if you are at work, contact your IT department.

Trojan Horse Warning

Hopefully, you will never see a pop-up message like the following:



Sygate Personal Firewall Pro 10/08/2001 00:03:52

Trojan Horse Warning

What Does This Mean?

This message indicates that **Sygate Personal Firewall Pro** has detected a known Trojan horse on your computer. It also explains that the Trojan horse has been blocked from accessing your network.

Detail

Again, clicking the **Detail** button will provide further information on the application's origins, file name, path, etc.

Why Did This Appear?

Either you tried to open the program identified as a Trojan horse, or it has been triggered by another program on your computer. It is possible that the Trojan was on your computer when you installed **Sygate Personal Firewall Pro**, or that you have recently downloaded it through a legitimate application, such as a web browser. The Trojan tired to access your network connection, and has been blocked by **Sygate Personal Firewall Pro.**

What Should I Do When I Receive a Trojan Horse Warning?

If at work, you should immediately notify your IT department. If you receive the notification on your home computer, you should purchase some anti-virus software. Some companies offer free trial versions of their anti-virus programs.

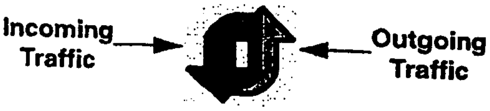
Getting Around Sygate Personal Firewall Pro

Understanding the different components of Sygate Personal Firewall makes it easy to navigate through the different screens and functions.

System Tray Icons

Once installed, **Sygate Personal Firewall** displays a small icon in your system tray (located on the right end of your task bar), consisting of two arrows. The arrows represent system traffic: the upward-pointing arrow is outgoing traffic; the downward-pointing arrow is incoming traffic.

These arrows give you a real-time update of your computer's traffic flow. You might not see a constant icon appearance for more than a few seconds, especially if you frequently use the Internet or your network connection.



System Tray Icon - Two Arrows

The colors of the arrows are always changing (as is the traffic flow on your computer). A table that lists all of the possible icon color combinations and their meanings appears in "Appendix 1", starting on page 72. For most users, it should be sufficient to remember the following points:

Table 2: System Icon Color Coding

If the color of the arrow is...	...then...
RED	...traffic is being blocked by the firewall.
BLUE	...traffic is flowing uninterrupted by the firewall.
GRAY	...no traffic is flowing in that direction.

ALERT MODE -FLASHING SYSTEM TRAY ICON

You might occasionally notice that the System Tray Icon begins flashing. This tells you that **Sygate Personal Firewall** is in Alert Mode. Alert Mode occurs when the firewall records an attempted attack on your computer. To view the attack information, double-click on the icon. The Security Log will open, displaying new log entries.

The icon will stop flashing after you double-click it. Please note that opening the Security Log through the main console will not cause the System Tray Icon to stop flashing.

USING THE SYSTEM TRAY ICON

You can easily configure basic aspects of **Sygate Personal Firewall Pro** without even opening the main console. Simply by double-clicking or right-clicking on the System Tray Icon, you can change your security level, view **Help** or log files, or even disable **Sygate Personal Firewall Pro**.

Table 3: System Tray Menu

Menu Option	What It will do for you...
Sygate Personal Firewall	Opens the Sygate Personal Firewall Pro main console.
Block All, Normal, Allow All	Choose one of the three security levels (for more on security levels, see "Setting Your Security Level", starting on page 39).
Applications	Opens the Applications List (for more on the Applications List, see "Applications List", starting on page 40).
Logs	Opens the Sygate Personal Firewall Pro Logs (for more on Logs, see "Logs", starting on page 46).
Options...	Opens the Options... window, for advanced security options (for more on the Options... window, see "Configuration Options", starting on page 55).
Hide System Tray Icon	Hides the System Tray Icon from view.
Help	Opens the embedded help files.
About	Opens the About window, providing information on your installation of Sygate Personal Firewall Pro.
Exit	Disables Sygate Personal Firewall Pro (option not available on Windows NT systems).

Hiding the System Tray Icon

The System Tray Icon is a very good way to remain updated on the status of your system security with **Sygate Personal Firewall Pro**. If, however, you do not like viewing the icon in the system tray, you can hide the icon from view. This is not recommended, since the System Tray Icon gives constant indication of your traffic flow and of attack attempts against your computer.

To Hide the System Tray Icon

There are two ways to hide the System Tray Icon:

•Click on the **Tools** menu. From the drop-down menu, click on **Hide System Tray Icon.**

•Open the **Tools** menu and select **Options....** On the **General Tab**, click to check the box next to the text **Hide Sygate Personal Firewall System Tray Icon.**

To UnHide the System Tray Icon

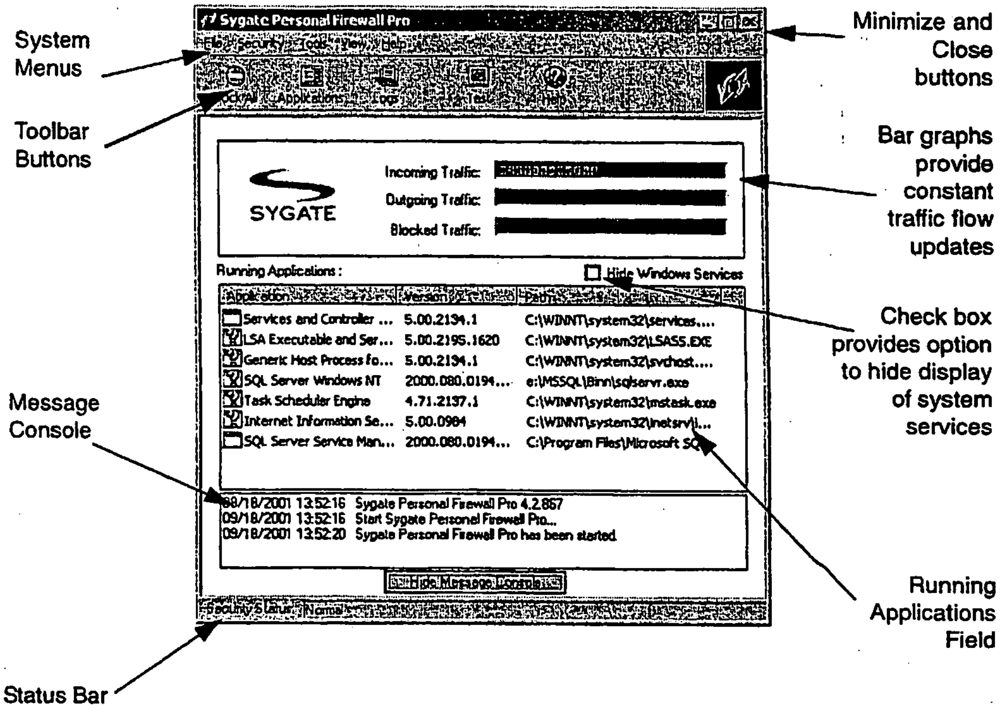
There are two ways to unhide the System Tray Icon:

•Click on the **Tools** menu. From the drop-down menu, click on **Hide System Tray Icon** so that the check mark next to it has disappeared.

•Open the **View** menu and select **Options....** On the **General Tab**, click to clear the box next to the text **Hide Sygate Personal Firewall System Tray Icon.**

MAIN CONSOLE

To open the **Sygate Personal Firewall Pro** main console, double-click the System Tray Icon, or right-click the System Tray Icon and select **Sygate Personal Firewall** from the list of options.



Application	Version	Path
Services and Controller ...	5.00.2134.1	C:\WINNT\system32\services....
LSA Executable and Ser...	5.00.2195.1620	C:\WINNT\system32\LSASS.EXE
Generic Host Process fo...	5.00.2134.1	C:\WINNT\system32\svchost....
SQL Server Windows NT	2000.080.0194...	e:\MSSQL\Binn\sqlservr.exe
Task Scheduler Engine	4.71.2137.1	C:\WINNT\system32\mstask.exe
Internet Information Se...	5.00.0984	C:\WINNT\system32\inetsrv\i...
SQL Server Service Man...	2000.080.0194...	C:\Program Files\Microsoft SQ...

```
08/18/2001 13:52:16  Sygate Personal Firewall Pro 4.2.867
09/18/2001 13:52:16  Start Sygate Personal Firewall Pro...
09/18/2001 13:52:20  Sygate Personal Firewall Pro has been started
```

Sygate Personal Firewall Pro Main Console

Traffic Flow Bar Graphs

The first thing you will probably notice about the main console is the set of horizontal bar graphs below the toolbar. These graphs provide real-time graphical representation of the traffic that is flowing in and out of your computer.

The top (green) graph represents traffic that is entering your computer from your network connection.

The next (blue) graph displays the traffic that is flowing out of your computer through a network connection.

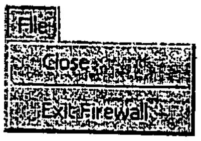
The bottom (red) graph shows traffic, flowing in either direction, that is being blocked by **Sygate Personal Firewall Pro** for security reasons.

Note Even if the main screen is not visible, **Sygate Personal Firewall Pro** is still running in the background.

Menus

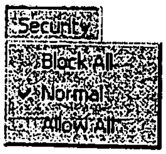
The main screen is designed to provide instant system status information, while displaying links and leads to other functions and features of **Sygate Personal Firewall Pro**. The top of the screen displays a standard menu with the following options: **File, Security Level, Tools, View,** and **Help.**

File



Clicking on the **File** menu opens a pull-down list with two choices: Close, which closes the main console, and **Exit Firewall,** which stops the **Sygate Personal Firewall Pro** service and disables firewall protection. To restart the service, you will need to reopen the firewall from the **Programs** menu under the **Start** menu.

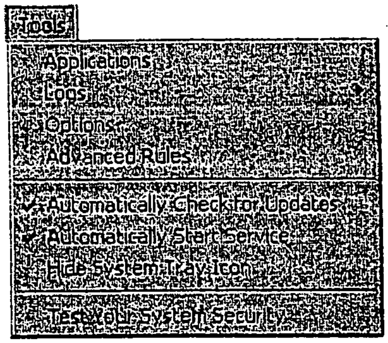
Security



In **Sygate Personal Firewall Pro**, there are three security levels that you can utilize: **Block All**, Normal, and **Allow All. Normal** is the default setting in **Sygate Personal Firewall Pro,** and is the security level that you will probably use the most. **Block All** and **Allow All** are used when you need to utilize the option either allowing or blocking all packets of information entering and leaving your computer.

Tools

The **Tools** menu provides several options. Selecting **Applications** opens the **Applications List**, a catalog of all the software applications that have attempted to access your network, as well as the level of trust you have associated with them (for more information on the **Applications List**, see the section "Applications List", starting on page 40).


Tools
Applications
Logs
Options
Advanced Rules
✓ Automatically Check for Updates
✓ Automatically Start Service
Hide System Tray Icon
Test Your System Security

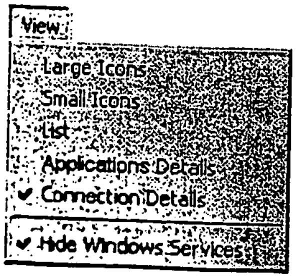
You can choose to view any of the four log files from the **Tools** menu (for information on viewing and understanding logs, see "Logs", starting on page 46).

The **Options** selection offers features including email alerts,. Network Neighborhood browsing rights, multiple NIC support, and log file configuration. See "Configuration Options", starting on page 55 to learn more about configuration features.

The **Advanced Rules** option offers a configuration window in which you can create rules that apply to all applications (see "Advanced Rule Configuration", starting on page 60).

A checklist on the **Tools** menu provides the options to automatically launch **Sygate Personal Firewall Pro** when your computer is booted, use SOS vulnerability assessment (see "Vulnerability Assessment", starting on page 67), hide the System Tray Icon, or disable the firewall altogether.

View



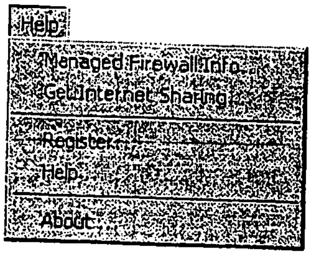
The **View** menu gives you the option to alter the display of software programs[1] in the **Running Applications** field. The option Large Icons displays 32x32 icons[2] in the field. The Small Icons option displays 16x16 icons. Both the large and small icon displays provide the full name of the application below the icon itself, and the icons are displayed in a "corkboard" fashion.

The List option also provides small icon representations, with the icons displayed in a standard list.

The Applications Details option provides not only a list of all running applications, but also useful information on the version number and location path of each application.

The Connection Details options gives further information on the type of connection being made by an each application accessing your network connection, as well as the protocol, local and remote ports and IP addresses being used, the application path, and more.

Help



The **Help** menu provides a link to the embedded Help file, the about window, and links to information on Sygate® Technologies Managed Firewall and Internet Sharing opportunities.

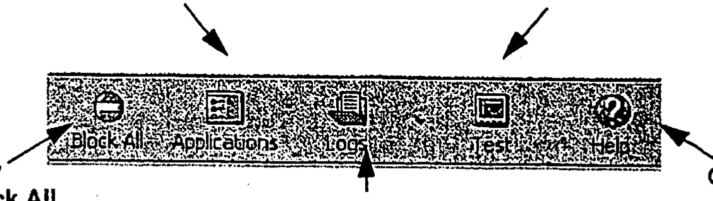
Toolbar Buttons

The buttons located below the menu items can be used to quickly access logs, view the **Help**

[1] These programs are applications that are currently accessing or attempting to access your network connection.

[2] Each icon represents a software application or a system service. Most icons should be familiar to you, although some may not.

file, or access Sygate® Technologies Online Services vulnerability assessment technologies.



Opens the Applications List for configuration of application-based security

Opens Sygate Online Services vulnerability assessment scans site.

Sets security level to **Block All**

Opens Sygate Personal Firewall Pro logs. By default, Security Log is opened

Opens SPF Pro Help files

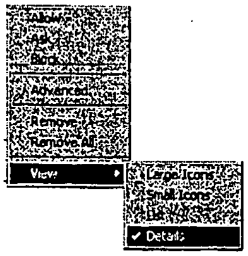
Sygate Personal Firewall Pro Toolbar Buttons

Running Applications Field

The **Running Applications** field is located directly below the traffic flow bars. It provides a real-time list of all applications and services that are currently accessing your network connection.

Applications and services are typically represented by their associated icons and names.

There are several different ways in which you can select to view the list of running applications and services. To change the view, open the **View** menu at the top of the main console and select the desired view.



Right-click anywhere in the Running Applications field

Alternately, you can right-click on any blank area inside the **Running Applications** field and select the desired view from the **View** pop-up list.

The view choices are **Large Icons**, **Small Icons**, **List**, **Application Details**, and **Connection Details**.

Table 4: View

View	What you'll see...
Large Icons	Large application/service icons representing with the name of the application/service, arranged in horizontal lines
Small Icons	Smaller icons and the application/service names, arranged in horizontal lines
List	Small icons and the application/service name, arranged in a vertical list
Application Details	A vertical list of icons and application/service names, with version and path information
Connection Details	Shows the details of each network connection made by an individual application or service
Hide Windows Services	Checking the box at the top of the **Running Applications** field will hide system services from being displayed

Regardless of the view you choose, the icons will display the application or service status in the **Running Applications** field. There are three application statuses in **Sygate Personal Firewall Pro**: Allow, Ask, and Block. You assign a status to an application or service when it attempts to access your network connection, and **Sygate Personal Firewall** opens a pop-up message asking if you wish to grant it access (for more information on application/service access, see the section titled "Applications List", starting on page 40).

A small graphic is displayed over the icon in the **Running Applications** field to indicate the status of the application or service.

Table 5: Application Status Icons

Icon	Status	Description
e	Allow	Icon appears normal, with no marks
e	Ask	Icon appears with a small, yellow question mark
e	Block	Icon appears with a red circle and cross-out mark

Message Console

The **Message Console** of **Sygate Personal Firewall** is located below the **Running Applications** field on the main console. It provides a real-time update of network communication, including profile downloads and service starting and stopping.

The **Message Console** is, by default, hidden from view. To view the Message Console, click the **Show Message Console** button below the **Running Applications** field on the main console. The **Message Console** will appear.

To hide the **Message Console** from view, click the **Hide Message Console** button. The **Message Console** will collapse so that only the **Show Message Console** button is apparent.

Status Bar

The **Status Bar** is located along the bottom of the main console, and offers real-time information regarding the security level that you have selected for **Sygate Personal Firewall Pro**.

Minimize and Close Buttons

You can hide the **Sygate Personal Firewall Pro** from view by clicking on the **Minimize** and **Close** buttons in the upper-right hand corner of the window.

Security Levels

Your security level is the main portion of your overall *security policy*, and determines the level of protection guaranteed to your computer.

In **Sygate Personal Firewall Pro**, your security level determines your overall approach to enforcing your computer's security. When you choose a security level, *you are selecting a security policy* that can be either highly flexible, extremely liberal, or iron-fisted. Going back to the nightclub example, after determining your overall policy and setup, your bouncers and security guards need to make careful security decisions based on a combination of data that you provide, and information they gather from scrutinizing guests. As the owner of one of the most desirable party locations, you would need the control to enforce a highly complex security policy, with the flexibility to immediately switch policies on a moment's notice.

There are three different security levels available with **Sygate Personal Firewall Pro**: **Normal**, which is a configurable security policy, **Block All**, which prevents any traffic from entering or leaving your computer, and **Allow All**, which allows a free flow of traffic to and from your computer.

Most users will find that they operate under the **Normal** security level for the majority of their computing time. Once you set **Normal** as your security policy, you can set access statuses (rights) to individual applications that try to access your network.

> **Note** No matter what security level you are operating under, you can configure settings for the **Normal** security level. For instance, if you are downloading a file that requires you to use the **Allow All** security level, you can configure the settings for the **Normal** security level during that time. However, the changes you make to the settings are applicable to the **Normal** security level, and will only take effect once you switch back to the **Normal** security level.

Normal

The **Normal** level is referred to as a "configurable" setting because, using the **Applications List** and **Advanced Application Configuration** features, you can arrange your policy within the **Normal** setting.

Individual applications and services can be assigned separate settings under the **Normal** security level. For instance, you can block some applications using certain ports during certain hours, while allowing other applications using specified protocols at all times.

Think of **Normal** as the kind of security policy you might need for moderate evenings at your nightclub: plenty of customers, highly suspicious bouncers, and a well-monitored overall complex. Within the **Normal** level, you have infinite security policy combinations available to you.

Individual applications, like individual guests, can be assigned access statuses based on different attributes. Let's say that your nightclub agenda for one evening is to let Cindy Crawford inside, regardless of what she is wearing or who she has brought with her, even if she arrives on a city bus. However, you instruct the bouncers not to let any of the local politicians in because, frankly, they don't tip well enough. Around 1 AM, when the club is getting crowded, you can instruct your bouncers to turn everyone down. You provide your bouncers with a detailed guest list including approved guest names and general instructions for dealing with the politicians.

You can configure similar rules and statuses for applications/services that try to get into or out of your computer. For instance, you can elect to allow your web browser unlimited access to and from your computer during your work hours every day, but prohibit it from accessing the network after 5 PM. At the same time, you can block media streaming applications and instant messaging services, except for a brief period during lunch, when they are both allowed. For information on access status configuration, see "Applications List", starting on page 40.

Note **Normal** puts your computer in stealth mode. Stealth mode makes your computer invisible to other computers on an external network, such as the Internet. You can use the Internet or network connection, but other users on the network, such as hackers roaming the Internet, will not be able to detect your computer.

Block All

Block All is the security level you would use if you suddenly decided that no more people should enter your nightclub. Either it's getting too crowded, or maybe you are having a problem with a rowdy guest inside.

In **Sygate Personal Firewall Pro**, **Block All** prevents any and all traffic from entering or leaving your computer. You should use this setting if you plan to be away from your computer for some time. Under the **Block All** setting, **Sygate Personal Firewall Pro** is still logging all traffic on your network connection.

Allow All

At your theoretical swanky nightclub, it is unlikely that you would relax security so much that anyone is allowed inside. However, there might come a time where you need to let more guests in. For instance, maybe traffic is slow one night, and you need more guests to liven up the party. You could instruct your bouncers to let everyone in. You would still be monitoring every movement on your security cameras, but wouldn't hinder the movement of guests in and out of the building.

Allow All should be used least of the three settings. Using the **Allow All** setting effectively disables **Sygate Personal Firewall Pro** blocking capabilities- any and all traffic attempting to access your network connection will be allowed, as if there is no firewall in place. However, even if **Sygate Personal Firewall Pro** is not blocking traffic, it is still logging all traffic that enters or leaves your system.

Disabling protection might seem like a strange type of security level. However, there are situations in which a firewall can disrupt the running of an application, such as an online game, or during rigorous downloading.

For these situations, you can use the **Allow All** setting. All traffic is still logged by **Sygate Personal Firewall Pro** under the **Allow All** setting, so that you can track potential security breaches or troubleshoot your system. *After you finish running the incompatible application, you should immediately return your status to* **Normal** *or* **Block All.**

You should use the **Allow All** setting very sparingly.

Setting Your Security Level

There are two ways to set your security level:

- Right-click on the **Sygate Personal Firewall Pro** System Tray Icon and select the level from the list.
- Open the **Sygate Personal Firewall Pro** main console. Open the **Security** menu and select the desired security level from the menu. You can switch to the **Block All** level by clicking the **Block All** button on the main console toolbar.

Note You can change your security level at any time using either of the methods described above.

Applications List

The Applications List is a list of "guests" that have tried to access your network connection, including those are allowed to use your network connection, blocked from using your network connection, or only allowed under certain conditions.

The **Applications List** is a roster that dictates application statutes in relation to **Sygate Personal Firewall Pro**. A list of applications (programs) and services that have been detected trying to access your network connection since the installation of **Sygate Personal Firewall Pro**, the **Applications List** is a useful area from which you can provide applications with the rules they need to act according to your wishes for them. This includes any applications that you have allowed or denied access to your network connection.

The **Applications List** provides a central location for you to assign an access status to each application/service that has tried to access your network. The status of an application determines when and how, if at all, an application can use your network connection.

Advanced status configuration settings allow you to specify which port an application can use, or to schedule a time period in which an application can be allowed or denied use of your network connection.

Note Don't confuse the Applications List (which displays a list of all applications that have attempted contact with your network connection since the installation of **Sygate Personal Firewall Pro**, and is opened in a new window from the main console) with the Running Applications field (which is located on the main console and shows all the applications that are *currently* accessing your network connection).

What is an Access Status?

An access status is a set of rules applied to an application or service that determine how and when, if at all, an application gets to use your network connection. There are three main access statuses: Allow, Ask, or Block.

Opening the Applications List

You can access the **Applications List** by clicking the **Applications** icon on the toolbar, or by selecting **Applications** under the **View** menu.

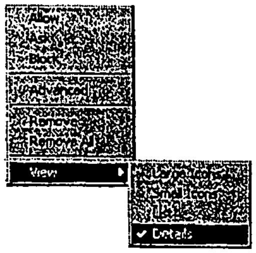
Viewing the Applications List

The **Applications List** shows all applications and services that have attempted to access your network connection since the installation of **Sygate Personal Firewall Pro**. The application/service name, version, access status, and path are provided in a simple screen.

Like the **Running Applications** field, you can change the display view for the applications and services shown in the **Applications List**. To change the view, right-click anywhere in the **Applications List**.

Select **View** from the list of options, then select the desired view. The different views are explained in the section entitled "Running Applications Field", starting on page 33.

To select an application or service for configuration, click on its icon, file name, version, access status, or path. Once the application or service name is highlighted, you can change or configure its access status, or remove it from the **Applications List**. See "Advanced Application Configuration", starting on page 43 for information on security settings options.

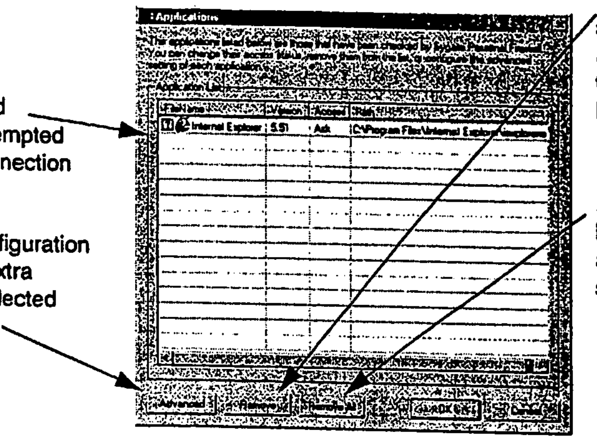


Selecting the view for Applications List

The buttons at the bottom of the **Applications List** screen provide the option to remove selected or all applications from the list. Once an application/service is removed from the **Applications List**, its access status is erased.

Once the application/service attempts to connect to the network again, you will be notified through a new application pop-up, and be asked to assign a new status to the application/

service.



List of applications and services that have attempted to access network connection

Opens Advanced Configuration window to configure extra security options for selected application/service

Removes the selected application from the Applications List

Removes all listed applications/ services from list

What is an Access Status?

An access status is a set of rules assigned to an application (or a system service) within **Sygate Personal Firewall Pro** that determines if, when, and how an application can access the user's network connection/modem. It is a sort of *Bill of Rights* for an application, specifying what rights to the network are given to an individual application. There are three application statuses in **Sygate Personal Firewall Pro**: **Allow**, **Ask**, and **Block**.

An application with a status of **Allow** will be allowed to access network connections, regardless of the source of the request.

An application with a status of Ask requires your permission each time it attempts to access network connections. For instance, if you assign the status of Ask to Internet Explorer, you will be asked to grant the application permission to utilize your network connection or modem every time Internet Explorer is opened.

An application with a status of **Block** will be blocked from using your network until you change its status. A blocked application cannot, under any circumstances, send data packets into or out of your computer.

For a chart of the graphical representations of application status in the **Running Applications** field, see "Running Applications Field", starting on page 33).

To Change the Status of an Application/Service in the Applications List

1. Open the **Applications List** by clicking on the **Applications List** icon, or opening the **Tools** menu and selecting **Applications.**

2. Click on the **File Name** of the appropriate application or service until the row is highlighted.

3. Using your mouse, right-click on the highlighted row.

4. Select the appropriate status (Allow, Ask, or Block) from the list.

5. Click **OK** to close the **Applications List.**

To Change the Status of an Application or Service from the Main Screen

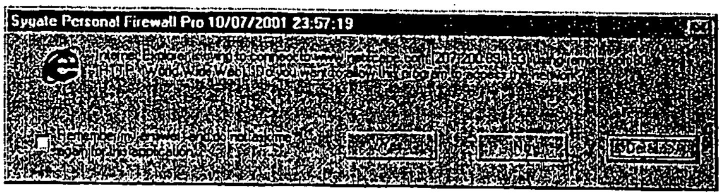
1. Right-click on the icon or application name of the application or service.

2. A pop-up menu will open, giving the options of Allow, Ask, or **Block**. Select one of the options by clicking on it.

3. The application icon will change to reflect the new status.

To Change the Status of an Application from Ask to...

When an application or service with the status of Ask tries to access your network connection, you will see a pop-up message similar to the one below.



Sygate Personal Firewall Pro 10/07/2001 23:57:19

[illegible]

- To change the status of this application to "**Allow**", check the box next to the message **Remember my answer, and do not ask me again for this application** and click **Yes.**
- To change the status of this application to "**Block**", check the box next to the message **Remember my answer, and do not ask me again for this application** and click **No.**

Advanced Application Configuration

You can configure advanced security settings for each application on your application list by setting certain restrictions on which IP Addresses and ports an application can utilize. Advanced configuration should only be undertaken by users who have a firm grasp on computer ports and application protocol.

To Set Advanced Configuration

1. Open the **Applications List** by clicking on the **Applications** icon on the **Sygate**

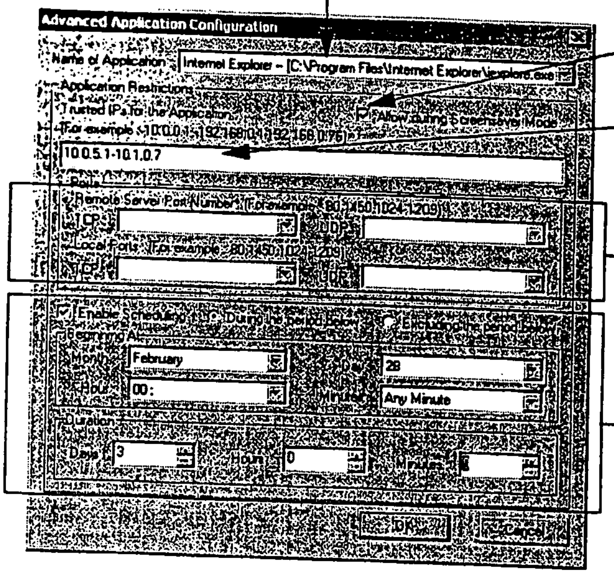
Personal Firewall Pro main console, or by right-clicking the System Tray Icon and selecting **Applications** from the list of choices.

2. Select the name of the application that you wish to configure advanced settings for.

3. Make sure the name of the application is highlighted.

4. Click the **Advanced** button at the bottom left corner of the **Applications List** screen.

5. The **Advanced Application Configuration** window opens.



Select application from pull-down list.

Check box to allow this application network access during Screensaver Mode.

Enter trusted IP address or address range for selected application

Enter trusted remote and local ports for the given protocols

Set scheduling either during or exuding specific time frames

Advanced Application Configuration

Name of Application: Internet Explorer -- [C:\Program Files\Internet Explorer\iexplore.exe]

Application Restrictions

Trusted IPs for the Application: ☑ Allow during Screensaver Mode

(For example: 10.0.0.1-192.168.0.1;192.168.0.76)

10.0.5.1-10.1.0.7

Ports

Remote Server Port Number (For example: 80;1450;1024-1209)

TCP: UDP:

Local Ports (For example: 80;1450;1024-1209)

TCP: UDP:

☑ Enable Scheduling ○ During the period below ○ Excluding the period below

Beginning At

Month: February Day: 28

Hour: 00: Minute: Any Minute

Duration

Days: 3 Hours: 0 Minutes:

Advanced Application Configuration

6. Make sure that the correct application in selected in the **Name of Application** pull-down list.

7. Decide if the application should be allowed network access during Screensaver Mode. Check the box next to the text Allow **during Screensaver Mode** to allow. Clear the box to

block the selected application during Screensaver Mode (for more information on Screensaver Mode, see "Screensaver Mode", starting on page 56).

8. Enter trusted IPs or IP ranges in the **Trusted IPs for the Application** text box.

   You must enter a valid IP address range. Please note that the following IP address ranges are invalid:

   •0.0.0.0

   •255.255.255.255

   •127.X.X.X

9. Enter the ports or ranges of ports that can be utilized for this application.

10. Click **OK** if the application restrictions are to be in effect constantly. If you wish to set a time limit or schedule specific periods when the restrictions will be in effect, see "Enable Scheduling" below.

To Enable Scheduling

You can also set times for which the advanced configurations take effect.

1. Check the **Enable Scheduling** check box below the **Ports** section on the **Advanced Application Configuration** screen.

2. Select either the **During the period below** or the **Excluding the period below** dial.

3. Select a Beginning Month, Day, Hour, and Minutes from the appropriate pull-down boxes.

4. Enter a duration in units of Days, Hours, and/or Minutes.

5. Click **OK** to set restrictions.

Logs

In Sygate Personal Firewall Pro, logs are like security cameras - they provide eyes at all different angles for comprehensive security, and offer the most comprehensive method of tracking attempted attacks on your computer.

Security guards usually keep detailed logs in order to have a record of each time period they work. If a crime occurs, or something is later discovered missing, the guard can look back at their records for clues about who might have committed the crime, and look for ways to prevent future problems.

Sygate Personal Firewall Pro is built with an detailed logging system that tracks the flow of traffic on and off of your computer. There are four types of logs in **Sygate Personal Firewall Pro**: **Security, System, Traffic,** and **Packet**. Each log is designed to monitor and record all information relevant to the maintenance of computer security. Logs provide a useful way to look back on a day's events, to see the attacks that **Sygate Personal Firewall** blocked, and to look for clues that might help build better security policies for a future of safe computing.

VIEWING LOGS

Understanding Logs

The four different logs provide varying sets of information. The **Security Log** records all attack attempts aimed at your computer that have been blocked by **Sygate® Personal Firewall™**. This includes port scans, denial of service attacks, etc. The **System Log** is a record of all activity surrounding **Sygate Personal Firewall Pro**, such as the starting and stopping of the firewall services. The **Traffic Log** records all network traffic, such as web sites that you visit. The **Packet Log**[1] captures all raw packet data that is recorded in the **Traffic Log.**

Opening Sygate Personal Firewall Pro Logs

- Right-click the System Tray Icon. Select **Logs**, then choose from the list of logs.
- From the main console, click the **Logs** icon. The **Security** log will open by default.
- From the main console, open the **Tools** menu. Select **Logs**, and then

[1] The Packet Log is, by default, disabled. To enable the Packet Log, see "To Capture Packet Log", starting on page 59.

choose the log that you wish to view.

Exiting Logs

•To close a log file, open the **File** menu and select **Exit**. Or, click the close button in the upper-right hand corner of the file window.

Log Setup

Sygate Personal Firewall Logs are constructed much like a normal, real-life security log. The log itself is recorded on a spreadsheet. Each "event", whether it be an attempted attack, or the initialization of an application or service, is recorded across a single line on a data sheet. The time and type of the event, source, severity, and other aspects are displayed in columns on the same line. The entire data sheet of events is called a **log file.**

The table below gives an three abbreviated examples of security log events. Each event is recorded on one line, with all information regarding the event displayed in individual columns.

Table 6: Log Example

Time	ID	Security Level	Remote Host IP	Hack Type	Traffic Direction
1/05/2001 20:23:47	202	Critical	10.0.1.78	0	Incoming
1/07/2001 21:05:06	202	Mild	192.168.0.2	0	Incoming
1/08/2001 23:08:55	202	Critical	10.0.4.167	0	Outgoing

The information recorded in each log is useful for tracking potential security risks, possible system problems, and network or connection issues.

Empty Log File?

Sometimes, when a file is opened, it appears to be empty.

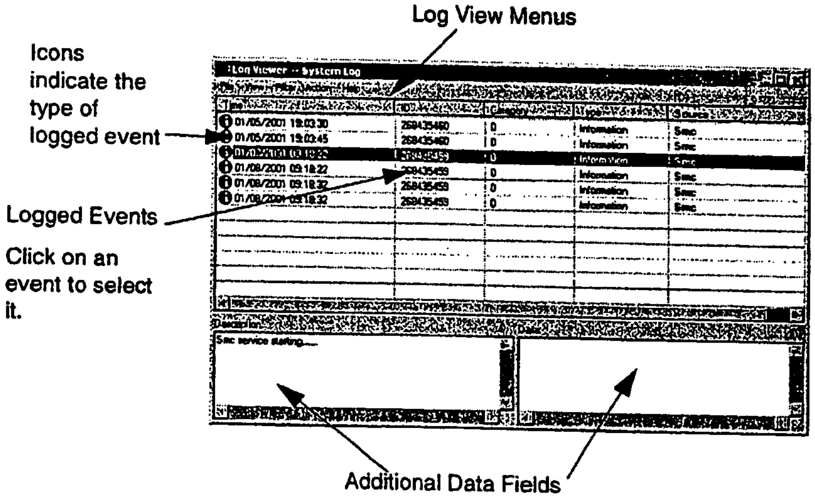
This is because the default view for log files contains only the current day's events. To view all events logged, open the **Filter** menu, and select **Show All Logs** from the list of options.

If you are viewing the Packet Log, and no log entries are displayed, you need to enable to Packet Log. See "To Capture Packet Log", starting on page 59 for more information.

Reading Log Files

Each log file opens in the **Log Viewer**, and provides a different set of information to help you deal with potential problems or trace hacking attempts. The sheer volume of information might seem kind of daunting initially, but once you start using them, logs will be one of your most useful defences against intruders.

The **Log Viewer** has several menus that can help you organize the information presented in the logs.


Log View Menus
Icons indicate the type of logged event
Logged Events
Click on an event to select it.
Additional Data Fields
Log Viewer -- System Log
File View Filter Action Help
Description
Data

Time	ID	Category	Type	Source
01/05/2001 19:03:30	268435460	0	Information	Smc
01/05/2001 19:03:45	268435460	0	Information	Smc
01/08/2001 09:18:22	268435459	0	Information	Smc
01/08/2001 09:18:22	268435459	0	Information	Smc
01/08/2001 09:18:32	268435459	0	Information	Smc
01/08/2001 09:18:32	268435459	0	Information	Smc

Smc service starting.....

Example of a System Log File

Log Icons

The most noticeable aspect of a log file is probably the icon that appears next to the date and time in the first column of a log event. These icons represent different information in different files.

Table 7: Security Log Icons

🛡 **Critical**	🛡 **Major**	🛡 **Minor**

In the Security Log, the icons represent the severity of the logged event.

Table 8: System Log Icons

Error	Warning	Info

In the System Log the icons show issues related to the **Sygate Personal Firewall** service.

Table 9: Traffic Log Icons

Incoming Allowed	**Outgoing Allowed**	**Direction Unknown Allowed**
Incoming Blocked	**Outgoing Blocked**	**Direction Unknown Blocked**

The Traffic Log icons indicate the direction of the flow of traffic for a logged event, as well as if the traffic was blocked or allowed to pass through. If no icon appears, then the direction of the traffic is unknown.

Table 10: Packet Log Icons

Packet Log Event

The Packet Log displays the same icon before every logged event. The Packet Log is, by default, disabled. To enable the Packet Log, see "To Capture Packet Log", starting on page 59.

Small Data Fields

The **Sygate Personal Firewall Log Viewer** displays logged events in a large data field. Below the main data field are two smaller fields, called **Description** and **Data** in the System, Security, and Traffic Logs, which provide additional information regarding the selected event log.

The **Description** field provides a definition of the logged event selected in the main section of the log viewer. For instance, a System Log entry might be described in the Description field as "Smc service is stopped".

In the Packet Log, these fields are called **Raw Packet Decode** and **Raw Packet Dump** (for more information on the Packet Log, "The Packet Log", starting on page 54).

Filtering Logs

By default, **Sygate Personal Firewall Pro** displays log events for the present day. The **Filter** menu allows you to select your view of logs based on time span or, for the System and Security Logs, by severity level.

Alternately, if you wish to view the log events for a limited time span, or based on severity level, you can limit your view of log events through the **Filter** menu. If you only want to view logs for a time period, or view only severe attacks on your computer, you can filter the types of logs on display.

To Filter a Log

1. From the open log, click on the **Filter** menu.

2. Select **1 Day Logs, 3 Day Logs, 1 Week Logs, 1 Month Logs**, or **Show All Logs.**

To Filter a Security Log

1. From the Log, open the **Filter** menu.

2. Select **1 Day Logs, 3 Day Logs, 1 Week Logs, 1 Month Logs**, or **Show All Logs.**

3. To view only critical attacks, open the **Filter** menu, then select **Severity**, and make sure that only the level **Critical** has a check mark beside it.

To Filter a System Log

1. From the System Log, open the **Filter** menu.

2. Select **1 Day Logs, 3 Day Logs, 1 Week Logs, 1 Month Logs**, or **Show All Logs.**

3. To filter by severity, open the **Filter** menu, then select and select which level(s) of severity you would like to view by placing a check mark next to the level. There are three severity levels for the System Log: Error, Warning, and Information.

Clearing Logs

If a log file becomes too large, you can delete the old entries. This isn't recommended, since log file information, however benign or repetitive in appearance, can help you or an administrator troubleshoot potential problems.

To Clear a Log File

There are two ways to clear a log file.

1. From the **Log Viewer**, open the **File** menu. Select **Clear**. Click **Yes** when the system asks if you wish to continue.

2. Open the **Options...** window from the **Tools** menu. Click on the **Log** tab. Click the **Clear Logs** button for each log that you wish to clear.

Refreshing Logs

If a log file remains open for an extended period of time, it will not display newly recorded items. To view updated log events in a file that has been open for more than five minutes, you will need to refresh the log. Please note that a log file will automatically refresh each time it is reopened.

To Refresh a Log File

1. From an open **Log Viewer**, click on the **View** menu.
2. Select **Refresh.**

Log Viewer Columns

Each log contains different information, labeled by different column headings. The meaning of the information in these columns are displayed in tables in "Appendix 2", starting on page 73.

Exporting Logs

All log files can be exported to another location to save space. Saved log files can serve as valuable information on the history of hacking attempts against your computer.

To Export a Log File

1. From the **Log Viewer**, open the **File** menu and select **Export....**
2. In the **Save As** window, provide a name for the saved log file. It is recommended that you incorporate the file type (Security, System, etc.) and the date in the name. Select a location to store the file.
3. Click **Save.**

Back Tracing

One of the most powerful tools of protection is information. **Sygate Personal Firewall** provides you with the information that you need to trace hack attempts and protect your computer and personal information from further intrusion attempts.

Back tracing enables you to pinpoint where data from a logged event has arrived from. Like retracing a criminal's path at a crime scene, back tracing shows the exact steps that incoming traffic has made before reaching your computer and being logged by **Sygate® Personal Firewall™.**

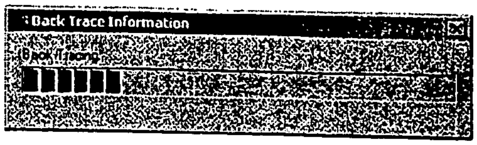
The option to backtrace a log event is available in both the Security and Traffic logs.

To Back Trace a Log Event

1. In an open log file, click on an event until it is highlighted.

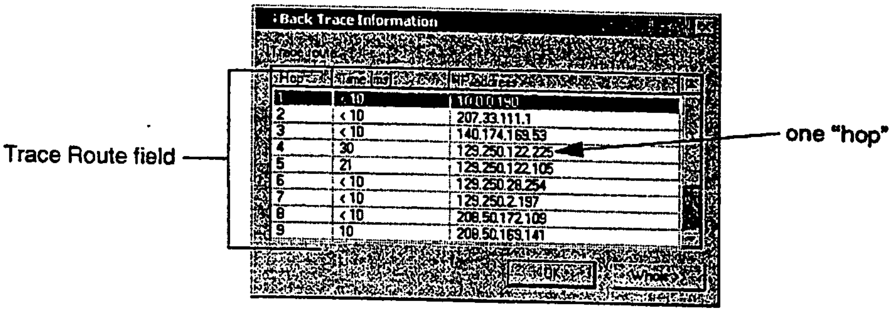
2. Right-click on the highlighted event. A pop-up window will offer the option to **Backtrace**.

3. Click on the **Backtrace** option. **Sygate Personal Firewall Pro** will begin backtracing the event.



Sygate Personal Firewall Pro back traces security log event.

4. The **Back Trace Information** window opens, displaying traced information on the IP addresses that the log event data visited before arriving at your computer's front door.

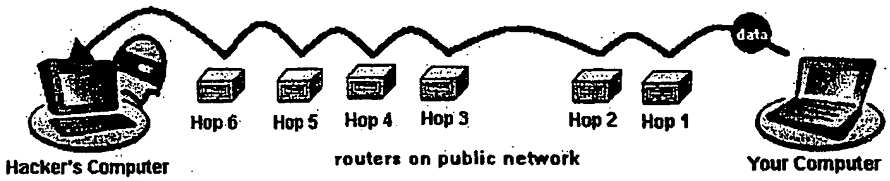


Hop	Time (ms)	IP address
1	< 10	10.0.0.190
2	< 10	207.33.111.1
3	< 10	140.174.169.53
4	30	129.250.122.225
5	21	129.250.122.105
6	< 10	129.250.28.254
7	< 10	129.250.2.197
8	< 10	208.50.172.109
9	10	208.50.169.141

Back Trace Information Window

The **Trace Route** field provides details on each "hop" made by the data packet that was logged by **Sygate Personal Firewall Pro**. A "hop" is a transition point, usually a router, that a packet of information travels through at as it makes its way from one computer to another on a public network, such as the Internet.

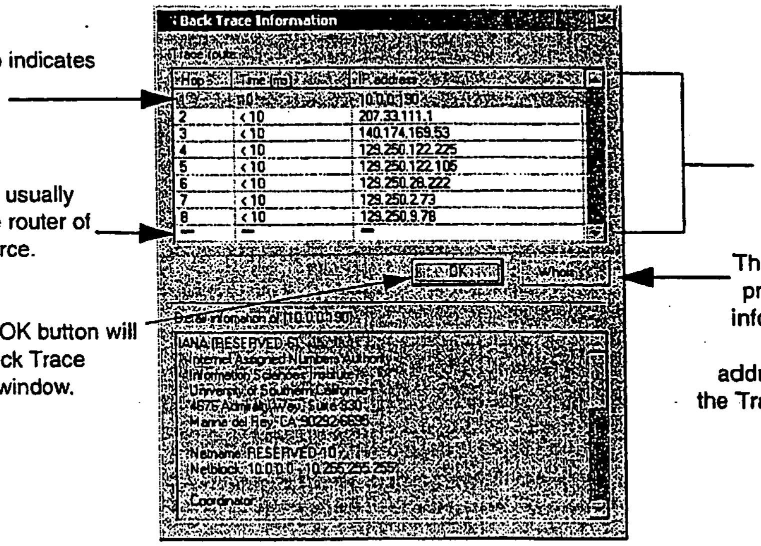
Backtracing is the process of following a data packet backwards, discovering which routers the data took in order to reach your computer. In the case of a Security Log entry, you can trace a data packet used in an attack attempt. Each router that a data packet passes through has an IP address, which is provided in the back trace **Trace Route** field.



Back tracing a Security Log entry

WhoIs

Clicking the **Whois** button prompts **Sygate Personal Firewall Pro** to pull up detailed information on each hop logged in the **Trace Route** field. The information is displayed in a drop-down **Detail Information** panel.



Hop	Time (ms)	IP address
1	0	10.0.0.190
2	<10	207.33.111.1
3	<10	140.174.169.53
4	<10	129.250.122.225
5	<10	129.250.122.105
6	<10	129.250.28.222
7	<10	129.250.2.73
8	<10	129.250.9.78
—	—	—

Detail information of [10.0.0.190]

```
IANA (RESERVED-5)
Internet Assigned Numbers Authority
Information Sciences Institute
University of Southern California
4676 Admiralty Way, Suite 330
Marina del Rey, CA 90292-6695

Netname: RESERVED-10
Netblock: 10.0.0.0 - 10.255.255.255

Coordinator:
```

The first Hop indicates your router

The last hop usually indicates the router of the data source.

Clicking the OK button will close the Back Trace Information window.

Trace Route field

The WhoIs button provides detailed information on the owner of the IP address selected in the Trace Route field.

Please note that the information provided in the **Detail Information** panel should be used responsibly. It is not advisable to contact persons listed in the **Detail Information** field unless you are experiencing a high number of security logs in which the attacks originate from one particular IP address.

Note You cannot use the **WhoIs** option if you are under the **Block All** security level. You must first switch to **Normal** or **Allow All**.

The Packet Log

The Packet Log is different from the other logs in **Sygate Personal Firewall Pro** in many ways. First, it is much larger. The Packet Log captures the actual raw packet *data* that travels through your network connection, as opposed to only recording the *incidence* of the data entering or leaving your computer.

This is significantly more information than some might expect. For instance, the simple act of opening an Internet browser causes **Sygate Personal Firewall** to log over two hundred entries in the Packet Log. A day's worth of Internet research can leave a user with a large number of Raw Packet Logs.

For this reason, the Packet Log is disabled by default in **Sygate Personal Firewall Pro**. You can enable Packet logging through the **Options...** window. Also, because of the large size of the Packet Log, you can configure a size or limit the number of days for which Packet Log data will be stored (see "Configuration Options", starting on page 55).

Raw Packet Decode and Raw Packet Dump Fields

Another trait unique to the Packet Log is the information provided in the small data fields beneath the main section of the **Log Viewer.** The **Raw Packet Decode** field provides details on the packet that was captured by **Sygate® Personal Firewall™**, such as the type of connection, the TCP and IP header data, the source and destination IP addresses, and the length of the packet. The **Raw Packet Dump** field contains the actual packet content in hexadecimal code, and information on configuration of the sender's IP address.

Configuration Options

The Options window is one of the most powerful security features of Sygate Personal Firewall Pro, offering a multitude of protection strategy options.

The **Options** selection of the **Tools** menu offers several settings for **Sygate Personal Firewall Pro**, including email notification of attacks, screen saver mode, log file configuration, and Network Neighborhood options.

To Open the Options Window

You can open the **Options...** window either from the **Tools** menu at the top of the main console, or by selecting it from the System Tray Icon pop-up menu. The **Options** window consists of four tabs: **General**, **Network Neighborhood**, **email Notification**, and **Log**.

The **OK** and **Cancel** buttons are located at the bottom of every tab in the **Options** window. The **OK** button applies any changes that you have made in the **Options** window, and then closes the window. Clicking the **Cancel** button ignores any changes you may have made in the **Options** window, and closes the window while retaining the previous settings.

General Tab

The **General** tab provides options for the basic running of **Sygate Personal Firewall Pro**.

Sygate Personal Firewall Pro Service

Checking this box automatically launches **Sygate Personal Firewall Pro** every time your computer is rebooted. This is the default setting. If you don't wish to have **Sygate Personal Firewall Pro** launch at start-up, clear this box of check marks.

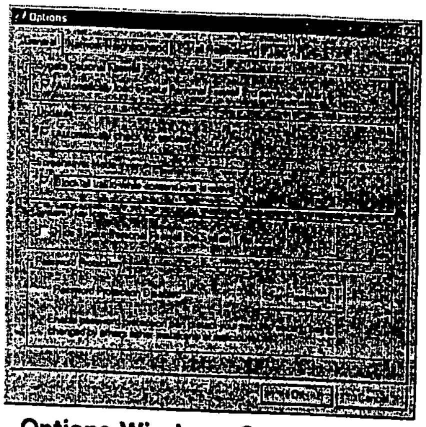
Updates

Enabling this feature allows **Sygate Personal Firewall Pro** to notify you of updates to **Sygate Personal Firewall Pro**. If you do not wish to be notified, clear this box of check marks.

Screensaver Mode

Enabling the Screensaver Mode option causes **Sygate Personal Firewall Pro** to switch the security level to **Block All** when your computer's screensaver is activated. As soon as the computer is used again, the security level will return to the previously assigned level. If you do not wish for your security level to change to **Block All** upon activation of your computer's screensaver, clear this box of all check marks.

You can allow certain applications network access during Screensaver Mode by checking the box at the top of the **Advanced Application Configuration** screen.



Options Window - General tab

System Tray Icon

Checking this box will hide the **Sygate Personal Firewall Pro** System Tray Icon from view. **Sygate Personal Firewall Pro** will still be running even if the System Tray Icon is hidden. The main console can be accessed by selecting `Start>Programs>Sygate Personal Firewall>Sygate Personal Firewall`. If you wish to view the System Tray Icon, clear this box of check marks.

You can also hide or unhide the System Tray Icon from the **Tools** menu on the main console of **Sygate Personal Firewall Pro**.

Password Protection

Enabling **Password Protection** will protect your settings from being changed by another user.

To Set a Password

1. To set a password for the first time, click the **Set Password...** button. The **Password** window opens.

2. Leave the **Old Password** field blank.

3. Enter a password in the **New Password** field, and type it again in the **Confirm New Password** field.

4. Click **OK**.

To Change an Old Password

1. To change your password, click the **Set Password...** button. The **Password** window opens.

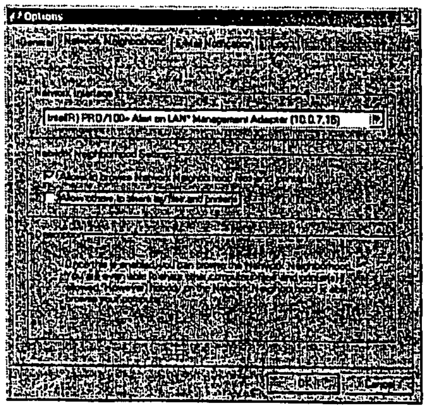
2. Enter your old password in the **Old Password** field. Enter a new password in the **New Password** field, and retype it in the **Confirm New Password** field.

3. Click **OK**.

NETWORK NEIGHBORHOOD TAB

The **Network Neighborhood** tab provides multiple interface support and network browsing rights configuration. The **Network Neighborhood** tab is made up of three sections: **Network Interface, Network Neighborhood Settings**, and **Description.**

The **Network Interface** section contains a pull-down box that lists all networks that have been detected by **Sygate Personal Firewall Pro.** The options in the **Network Neighborhood** section apply to the network selected in the **Network Interface** pull-down box. The **Description** section offers a brief statement about the conditions that will be set according to which of the options you select from the **Network Neighborhood** section.



Network Interface

Intel(R) PRO/100+ Alert on LAN* Management Adapter (10.0.7.16)

Network Neighborhood Settings

☑ Allow to browse Network Neighborhood files and printer(s)

□ Allow others to share my files and printer(s)

Network Neighborhood Tab

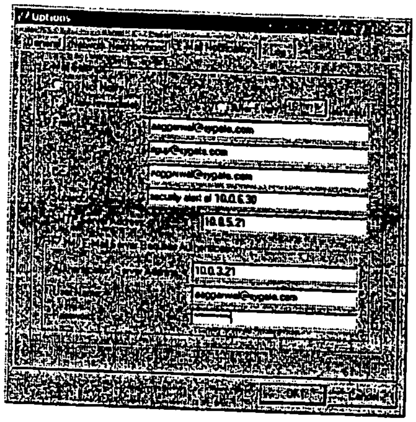
To Configure Network Neighborhood Rights

1. Select the network from the **Network Interface** pull-down list.

2. Decide if you wish to browse other computers on the network and if you wish to allow other users on the selected network to browse your computer. Under the **Network Neighborhood Settings** section, select the appropriate check boxes:

- •Selecting the **Allow to browse Network Neighborhood files and printer(s)** option will permit you to browse the files and printers on the selected network.
- •Selecting the **Allow others to share my files and printer(s)** will allow other users of the selected network to browse your files and use your printer(s).

EMAIL NOTIFICATION TAB



security alert at 10.0.6.30

10.0.5.21

10.0.3.21

Email Notification Tab

The **email Notification Tab** provides you with the option to automatically notify a specified recipient via email of any attacks against your computer.

To Activate email Notification

1. First, select the frequency of notification. You have three choices.
   - Select **Do Not Notify** to disable the email notification option.
   - Select **Notify Immediately** to have an email sent immediately following an attack on your computer.
   - Select **After Every X minutes** to have notification of security alerts sent at specified intervals.

2. Enter an email address in the **From:** address field. This can be your personal email address or another email address.

3. Enter a recipient email address in the **To:** field. This can be an administrator's email address, or your email address, if you are accessing email remotely.

4. If you wish, you may send a courtesy copy of each email to a specified email address in the **Cc:** field.

5. Enter a subject in the **Subject** field.

6. Enter your SMTP Server Address.

7. If your email server requires authentication, click to check the box next to the indicative text. Enter the address of the authentication server in the **Authentication Server Address** field.

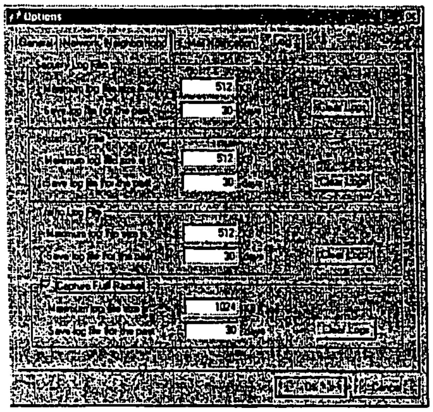
8. Enter your username and password for the authentication server in the appropriate fields.

9. Click **OK** to save changes.

Log Tab

The **Log** tab provides a central location to manage the logs for **Sygate Personal Firewall Pro**. The **Log** tab can also be reached through the **Log Viewer**, by opening the **File** menu and selecting **Options....**

Each log file is represented in a separate section in the **Log** tab. You can determine the standard log size for each log, as well as specify how many days worth of entries are recorded in each log.



Log Tab

To Set Log Size

1. Click on the appropriate **Maximum Log File Size** field for the log you wish to configure.

2. Enter a number. Click **OK.**

To Set Log Time Period

1. Click on the appropriate **Save Log File for the Past** field for the log you wish to configure.

2. Enter a number of days. Click **OK.**

To Clear Log

To clear a log from the **Log File** tab, simply click the **Clear Logs** button for the log you wish to clear.

To Capture Packet Log

1. Click to check the box next to the **Capture Packet Log** option.

2. Select a maximum file size (1024 KB is the default setting).

3. Enter a number of days for which **Sygate Personal Firewall Pro** should save the log file entries.

4. Click **OK.**

Advanced Rule Configuration

Sygate Personal Firewall Pro offers users the unique option to configure advanced rules that can override the rules automatically created by the firewall during normal user-firewall interaction. You may not realize it, but every time you allow or deny access to an application, you are creating a rule for that application. If you use Advanced Configuration to specify application access rights (such as scheduling and port rights), you are specifying parameters for the selected application, and thus creating an application rule. However, these rules are application-specific, so that if you create a schedule for an application, the schedule applies **only to that application.**

Advanced rules, on the other hand, are rules that you can create directly that affect all applications. If you create an advanced rule that blocks all traffic between 10 PM and 8 AM, the rule will override all other schedules and configurations that have been set for each application.

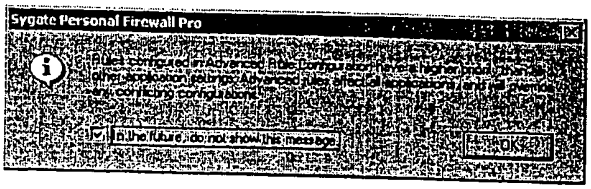
Rules in the **Advanced Rules** window will apply to all applications. Advanced rule configuration is available for users who wish to create universal rules for **Sygate Personal Firewall Pro.**

Creating Rules

When you create a universal rule, first decide what effect you want the rule to have.

Do you want to block all traffic when your screensaver is on? Would you like to allow all traffic from a particular source? Do you want to block UDP packets from a web site?

1. To begin, open the **Tools** menu at the top of the main console, and select **Advanced Rules**. You will most likely see the following message:



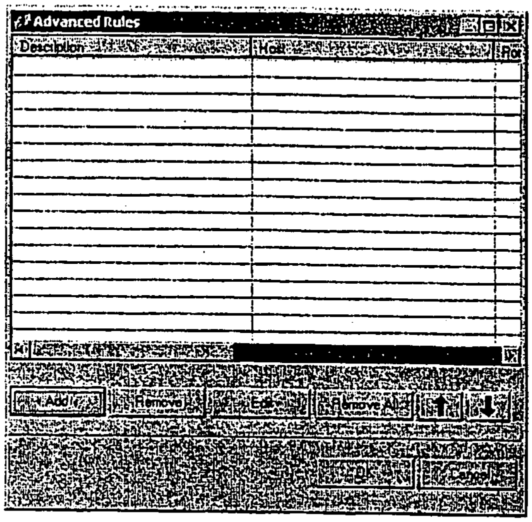
Sygate Personal Firewall Pro

Rules configured in Advanced Rule Configuration have a higher priority than all other application settings. Advanced rules affect all applications, and will override any conflicting configurations.

☑ In the future, do not show this message

2. This message explains that rules in the **Advanced Rules** window will override any other automatic rules in **Sygate Personal Firewall Pro.**

3. The **Advanced Rules** window will open.



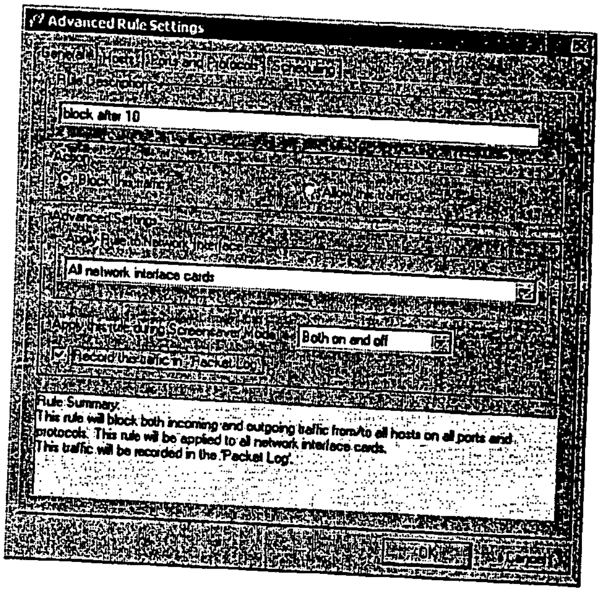
4. Once you have created rules, they will appear in this list.

5. Click the **Add** button. The **Advanced Rule Settings** window opens.

To create a rule, you must first specify the kind of traffic, and the conditions that must exist for the rule to take effect. There are four different sections within the **Advanced Rule Settings** window where you can specify the characteristics of the traffic: **General, Hosts, Ports and Protocols**, and **Scheduling.** You can use as many sections as necessary to specify the conditions and characteristics (time of day, type of traffic, port number) that will cause the rule to take effect, as well as the effect the rule will have. The more information and characteristics that you enter in the **Advanced Rule Settings** window, the more specific the rule will be. Note that each tab that contains specified information contributes to the functioning of a rule.

General Tab

The **General** tab is used to provide a name for the rule you are creating, as well as the effect that the rule will have (allowing or blocking traffic).



Rule Description: block after 10

Apply Rule to Network Interface: All network interface cards

Apply this rule during Screensaver Mode: Both on and off

☑ Record this traffic in Packet Log

Rule Summary:
This rule will block both incoming and outgoing traffic from/to all hosts on all ports and protocols. This rule will be applied to all network interface cards.
This traffic will be recorded in the 'Packet Log'.

General Tab

1. First, enter a rule description. This will also function as the name of the rule, and it should indicate qualities of the rule. For instance, "Rule1" may not be a very good name for a rule, but "Block After 10 PM" would be (assuming the rule had some sort of function that did block traffic after 10 PM).

2. Second, decide the main action of the rule - do you want to block traffic, or allow traffic?

3. Next, choose which network interface card this rule will apply to. If you have multiple network cards, select one from the pull-down list, or select All network interface cards to apply the rule to ever card.

4. Decide if this rule will be influenced by the activation of your computer's screensaver (if applicable).

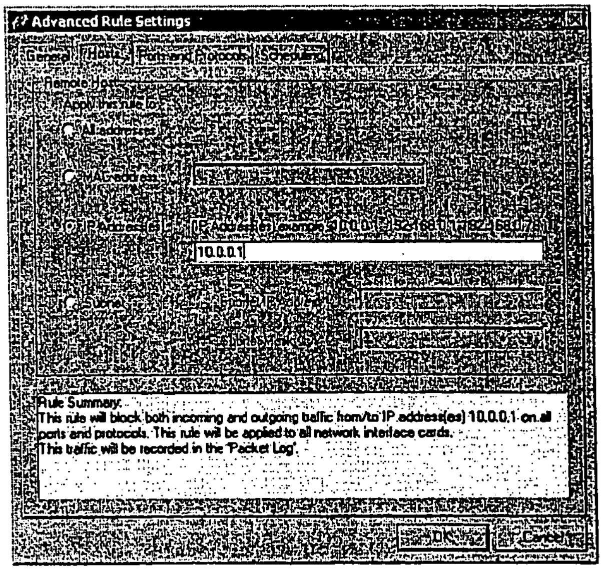
- On - The rule will be activated only when the screensaver is on. This is a great feature if you want to block all traffic and all ports while you computer is idle.
- Off - This rule will be activated only if the screen saver is off and all other conditions are satisfied.
- Both On and Off - This rule is unaffected by the screensaver.

5. Place a check in the **Record this traffic in 'Packet Log'** checkbox if you want traffic affected by this rule to be entered in the Packet Log.

6. The **Rule Summary** field at the bottom of the tab provides a summary of the rule's functionality. Click **OK** to set the rule, or click on another tab to further specify rule conditions and properties.

Hosts Tab

The **Hosts** tab is where you can specify the source (IP address, MAC address, or Subnet range) of traffic that you wish to block or allow.



10.0.0.1

Rule Summary:
This rule will block both incoming and outgoing traffic from/to IP address(es) 10.0.0.1 on all ports and protocols. This rule will be applied to all network interface cards.
This traffic will be recorded in the 'Packet Log'.

Hosts Tab

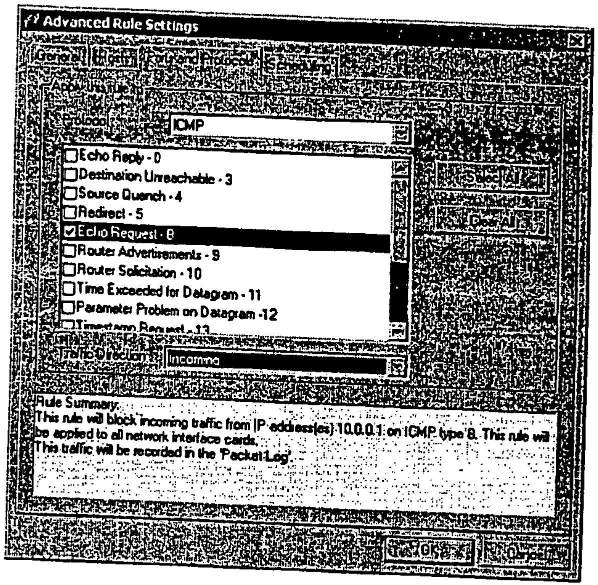
1. Select the way in which you want to identify the traffic source. You can use the **All Addresses** option if you are planning on blocking traffic from all sources for this rule.

2. Enter the corresponding address or address range.

3. The **Rule Summary** field at the bottom of the tab provides a summary of the rule's functionality. Click **OK** to set the rule, or click on another tab to further specify rule conditions and properties.

Ports and Protocols Tab

The **Ports and Protocols** tab provides an area to specify which ports and protocols, if any, should be affected by the traffic specified in the rule.



Protocol: ICMP

□ Echo Reply - 0
□ Destination Unreachable - 3
□ Source Quench - 4
□ Redirect - 5
☑ Echo Request - 8
□ Router Advertirements - 9
□ Router Solicitation - 10
□ Time Exceeded for Datagram - 11
□ Parameter Problem on Datagram -12
□ Timestamp Request - 13

Traffic Direction: Incoming

Rule Summary:
This rule will block incoming traffic from IP address(es) 10.0.0.1 on ICMP type 8. This rule will be applied to all network interface cards.
This traffic will be recorded in the 'Packet Log'.

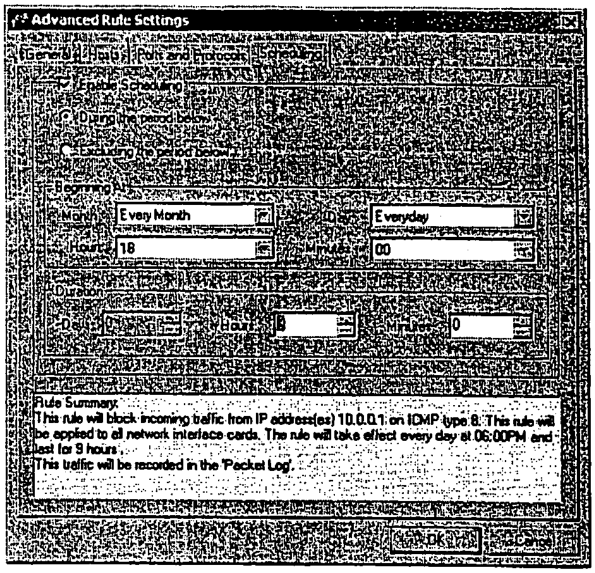
Ports and Protocols Tab

1. Select a protocol from the top pull-down box. Select **ALL** if you want the rule to apply to all protocols. You can also choose TCP, UDP, ICMP, or IP Type.
2. Then, select the traffic direction from the pull-down list.
3. The **Rule Summary** field at the bottom of the tab provides a summary of the rule's functionality. Click **OK** to set the rule, or click on another tab to further specify rule conditions and properties.

Scheduling

Scheduling is a good way to create a rule that you want to take effect only during (or excluding) certain time periods. For instance, if you want to block all traffic after 10 PM, then you can create a schedule that will permit the rule to do so.

1. Open the **Scheduling** tab. Place a check in the **Enable Scheduling** checkbox.



Month: Every Month

Day: Everyday

Hours: 18

Minutes: 00

Days: 0

Hours: 9

Minutes: 0

Rule Summary:
This rule will block incoming traffic from IP address(es) 10.0.0.1 on ICMP type 8. This rule will be applied to all network interface cards. The rule will take effect every day at 06:00PM and last for 9 hours.
This traffic will be recorded in the 'Packet Log'.

Scheduling Tab

2. Decide if you want the schedule to take place during a certain time period, or outside of a certain time period. Select either **During** or **Excluding**.

3. Select a month, day and beginning time from the pull-down lists, or leave the default settings, which will apply the rule schedule to all day, every day, all year.

4. If you have a beginning time, enter a duration for the rule's effect.

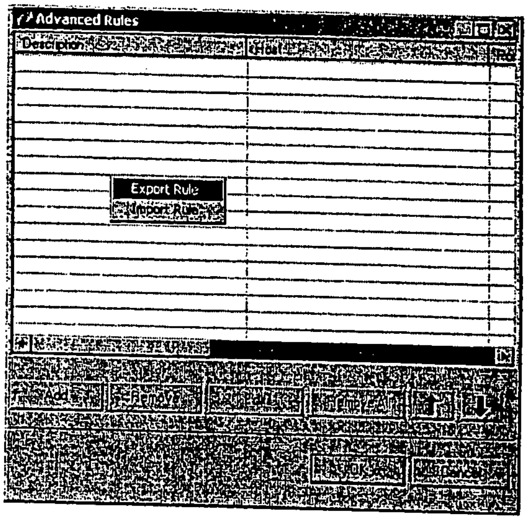
5. The **Rule Summary** field at the bottom of the tab provides a summary of the rule's functionality. Click **OK** to set the rule, or click on another tab to further specify rule conditions and properties.

Importing and Exporting Rules

You can import and export advanced rules to improve your security and computing functionality.

Importing a Rule

1. To import a rule, right-click anywhere in the **Advanced Rules** window rule list. The **Import/ Export** pop-up menu will appear.



Importing/Exporting a Rule

2. Select **Import Rule**. The **Import** window will open. Browse through the folders until you locate the rule that you would like to import. Click **Open.**

Exporting a Rule

1. To export a rule, right-click on the rule name in the **Advanced Rules** window. The **Import/ Export** pop-up menu will appear.

2. Select **Export Rule**. The **Export** window will open. Browse through the folders until you determine the location to which you will export the rule. Click **Save.**

Vulnerability Assessment

Reacting to hacking attacks is only one way of approaching computer security. A more comprehensive approach includes not only tracking attempted or successful attacks, but also preempting them - and vulnerability assessment is the key to preventing hackers from being successful.

SOS Scans

Intrusion detection is, by itself, a purely reactive security method. Users and administrators need to be proactive in their quest to block potential intruders and protect vital information. One of the most important ways to know that your security policies are working is to test your firewall.

Sygate® Technologies, Inc. has developed Sygate® Online Services (SOS) Security Scan, an online vulnerability assessment tool that can help users proactively locate weak points in their computer systems. This service is located at http://scan.sygate.com, and can be accessed through the **Sygate Personal Firewall Pro** main console. There are six main scanning options that can be utilized to assess possible security holes that compromise computer safety.

To Access Sygate® Online Services

1. Click the **Test** button located on the main console of **Sygate Personal Firewall Pro**, or select **Test Your System Security** from the **Tools** menu.

2. The Sygate® Technologies web page (http://scan.sygatech.com) will load, and the **Sygate® Online Services** scanner will attempt to determine your IP address, operating system, and web browser.

Six Different Scans

There are six different scans available through Sygate® Online Services, listed along the left side of the main scan page. To view a brief description of the scan, click the name once. The description will load on the right side of the screen.

To utilize a scan, click on the name of the scan and then click the **Scan Now** button.

A brief document of frequently asked questions about Sygate® Online Services can also be accessed from the main scan page, by clicking link labeled **Scan F.A.Q.** at the bottom, left hand side of the screen.

Quickscan

Quickscan is a brief, general scan that encompasses several scan processes. The Quickscan feature usually takes 20 seconds or less to accurately scan your computer's ports, protocols, and services for possible trojans and security holes. Quickscan will be recorded in **Sygate® Personal Firewall™**'s Security Log.

Stealth scan

Stealth scan scans your computer using specialized stealthing techniques, which mimic portions of legitimate computer communication in order to detect the presence of a computer. The Stealthscan takes about 20 seconds to complete, and will most likely not be recorded in the Security log.

Trojan scan

The Trojan scan ports commonly used by trojans for active trojan horse programs that you or someone else may have inadvertently downloaded onto your computer. The Trojanscan takes about 10 minutes to complete. A list of common Trojans is available on the web site.

TCP scan

The TCP scan examines the ports that are mainly reserved for TCP services, such as instant messaging services, to see if these ports are open to communication. Open ports indicate a dangerous security hole that can be exploited by malicious hackers.

SOS TCP scan will scan devices such as routers and proxies for users connecting to the web site through such a device. The scan takes roughly 20 minutes to complete and is logged by **Sygate Personal Firewall Pro** as a scan event in the Security Log.

UDP scan

The UDP scan uses various methods and protocols to probe for open ports utilizing UDP. SOS UDP scan will scan devices such as routers and proxies for users connecting to the web site through such a device. The scan takes about 10 minutes and should be logged in the Security log as a portscan from **Sygate®**.

ICMP scan

The ICMP scan probes for ports that normally answer ICMP inquiries. If no response is received from these ports, they are considered blocked.

When an SOS scan has completed scanning a user's computer, it will display a page with the results of the scan. If a user is running **Sygate Personal Firewall Pro**, all scans should be blocked.

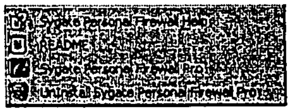
Uninstalling Sygate® Personal Firewall Pro™

There may come a time when you need to uninstall Sygate Personal Firewall Pro in order to install a newer version, or to install software incompatible with Sygate Personal Firewall Pro.

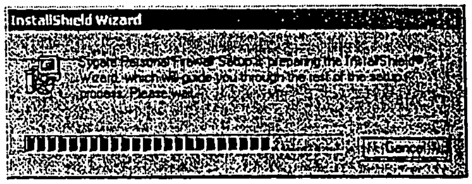
Although we have no idea as to why you might want to do this, there might come a time when you wish to uninstall **Sygate Personal Firewall Pro** from your computer.

Sygate Personal Firewall Pro can be uninstalled via the standard Windows procedure, using the **Add/Remove Programs** window under **Settings.** However, you can also use the following procedure:

1. Select **`Start>Programs>Sygate Personal Firewall>Uninstall Sygate Personal Firewall.`**

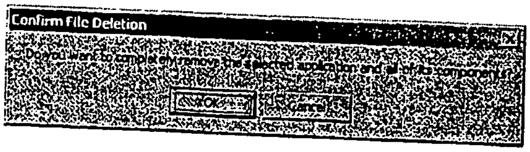

Sygate Personal Firewall Help
README
Sygate Personal Firewall Pro
Uninstall Sygate Personal Firewall Pro

2. The **InstallShield Wizard** will begin uninstalling.



Sygate Personal Firewall Setup is preparing the InstallShield® Wizard which will guide you through the rest of the setup process. Please wait.

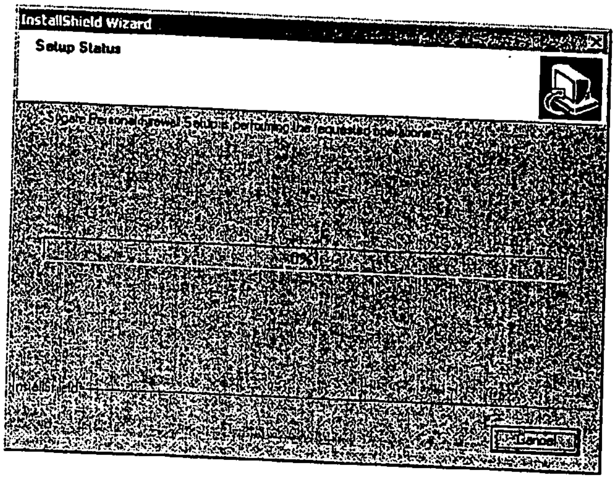
3. Click **OK** when the **Confirm File Deletion** screen pops up.



Confirm File Deletion

Do you want to completely remove the selected application and all of its components?

4. **InstallShield Wizard** will begin uninstalling **Sygate Personal Firewall Pro.**

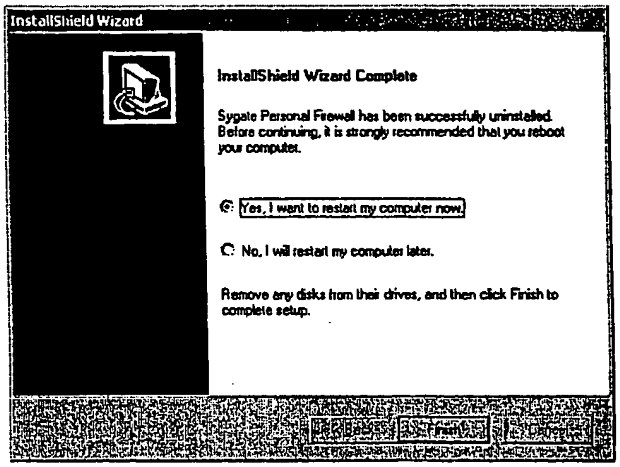


InstallShield Wizard

Setup Status

Sygate Personal Firewall Setup is performing the requested operations.

5. **InstallShield Wizard** will complete file deletions. Select **Yes** and then **Finish** to restart your computer.



InstallShield Wizard

InstallShield Wizard Complete

Sygate Personal Firewall has been successfully uninstalled. Before continuing, it is strongly recommended that you reboot your computer.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

Appendix 1

The table below illustrates the different appearances that the **Sygate Personal Firewall Pro** System Tray Icon may have, and what they mean.

Table 11: System Tray Icons

Icon	Meaning
	Sygate Personal Firewall Pro is in Alert Mode. This means that an attempted attack against your computer has been recorded in your Security Log. To make icon stop flashing, double-click on the icon. The Security Log will open, displaying new log entry.
	Incoming traffic is flowing uninterrupted; there is no outgoing traffic.
	Both incoming and outgoing traffic are flowing uninterrupted.
	There is no incoming traffic; outgoing traffic is flowing uninterrupted.
	Incoming traffic is blocked; outgoing traffic is flowing uninterrupted.
	Incoming traffic is blocked; there is no outgoing traffic.
	Both incoming and outgoing traffic are blocked.
	There is no incoming traffic; outgoing traffic is blocked.
	Incoming traffic is flowing uninterrupted; outgoing traffic is blocked.
	No traffic is flowing in either direction.

Appendix 2

The following tables provide descriptions of the information recorded in **Sygate Personal Firewall Pro** logs.

Table 12: System Log

Column Heading	What the Info Means...
Time	The date and time that the event was logged.
Type	The type of event - this will be either Error, Warning, or Information. An Error log indicates a problem with the source, a Warning log indicates a potential problem, and an Information log merely provides information on an event involving **Sygate Personal Firewall Pro.**
ID	The ID assigned to the event by **Sygate Personal Firewall Pro.**

Table 13: Security Log

Column Heading	What the Info Means...
Time	The exact date and time that the event was logged.
Security Type	Type of hacking attempt, such as Port Scan, Denial of Service, Trojan horse, etc.
Severity	One of three levels - Critical, Major, and Minor.
Count	Number of attacks logged.
Direction	Incoming or Outgoing - most attacks are Incoming, that is, they are originating from another computer and are attempting to enter yours. Other attacks, however, like Trojan horses, are programs that you might download onto your computer that then attack from within your computer, and are considered Outgoing.
Protocol	The type of protocol used in the attempted attack - TCP, UDP, ICMP.
Application Involved	This column provides the name and path of the application involved in the log event.
Remote IP	The IP address of the attempted attack source.
Remote Host Name	Name of the remote computer.
Local IP	Your IP address.
Begin Time	The time that the attack attempt began.
End Time	The time that the attack attempt ended.

Table 14: Traffic Log

Column Heading	What the Info Means...
Time	The exact date and time that the event was logged.
Protocol	Type of protocol - UDP, TCP, ICMP.
Direction	Which way the traffic was moving: into your computer (Incoming) or out of your computer (Outgoing)
Action	Action taken by **Sygate Personal Firewall Pro**: Blocked or Allowed.
Count	Number of events that occurred in this time period.
Application Involved	This column provides the name and path of the application involved in the security attack.
Remote Host IP	The IP address of the host computer.
Remote Host Name	Name of the host computer.
Remote Port	Port used by application.
Local IP	Your IP address.
Local Port	Port used on your computer for this traffic.
Begin Time	The beginning time of the event.
End Time	The time the event ended.
Rule Name	The rule that determined the passing or blockage of this traffic. If you were blocking certain applications, this column might read "Block_All". If **Sygate Personal Firewall Pro** is running at the Normal security level, this might read "Ask all running apps".

Table 15: Packet Log

Column Heading	What this Info Means...
Time	The exact date and time that the event was logged.
Remote IP	The IP address of the sender or recipient of the data being logged.
Remote Host Name	The name of the host computer.
Remote Port	The virtual port being used for this data.
Local IP	Your IP address.
Local Port	The port being accessed for this data.

Index